Document Number 102-95-014U

Final Report:

Results of the SBIR Phase II Effort

Contract No. N00039-93-C-0099
CDRL No. A003

September 5, 1995

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.

9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

TEL: (619) 546-8616
FAX: (619) 546-0814

Approved for public release; distribution is unlimited.

1995 0999 187

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 5, 1995	Final

4. TITLE AND SUBTITLE

Technical Report
Final Report: Results of the SBIR Phase II Effort

5. FUNDING NUMBERS

Contract No:
N00039-93-C-0099

6. AUTHOR(S)

Kym Blair

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

8. PERFORMING ORGANIZATION REPORT NUMBER

102-95-014U

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71CE)
Arlington, VA 22245-5200

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement: Approved for Public Release; Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort consisting of a series of analyses that extend the Phase I effort. This Final Report summarizes the results of those analyses. The Phase II effort consisted of the following tasks:

- Task 1 – Demonstration of Phase I Concept
- Task 2 – Navy Security Standards and Applications Analysis
- Task 3 – Analysis of End-to-End Encryption and Traffic Flow Confidentiality Options
- Task 4 – Naval Network Security Requirements Analysis
- Task 5 – NetWare Administrator's Security Guidance Handbook
- Task 7 – Participate in Security Groups.

In response to changing needs of the Navy, Phase II was redirected from a technical perspective with a focus on communications security technology to a "hands-on" perspective with a focus on network security Administration. The Novell NetWare Security Administrator's Security Guidance Handbook was the result of that redirection. The importance of this redirection has been recognized and will be carried into Phase III with the development of a comprehensive set of network security administration tools. In addition, the scope will be broadened to include support of Microsoft Windows NT security administrators as well.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	88
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	

Document Number 102-95-014U

Final Report:

Results of the SBIR Phase II Effort

Contract No. N00039-93-C-0099
CDRL No. A003

September 5, 1995

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 71)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.

9404 Genesee Avenue, Suite 237
La Jolla, CA 92037

TEL: (619) 546-8616
FAX: (619) 546-0814

Approved for public release; distribution is unlimited.

This Page Intentionally Left Blank

Table of Contents

Appendices

Index of Figures

A-1

This Page Intentionally Left Blank

Executive Summary

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort consisting of a series of analyses to extend the Phase I effort. This Final Report summarizes the results of those analyses. The Phase II effort consisted of the following tasks:

- Task 1 – Demonstration of Phase I Concept
- Task 2 – Navy Security Standards and Applications Analysis
- Task 3 – Analysis of End-to-End Encryption and Traffic Flow Confidentiality
- Task 4 – Naval Network Security Requirements Analysis
- Task 5 – NetWare Administrator's Security Guidance Handbook
- Task 6 – Provide Briefings for Phase III Support (canceled)
- Task 7 – Participate in Security Groups.

The first four tasks focused on security services and mechanisms in communications protocols, and on communications security requirements in military environments. In response to changing needs of the Navy, Phase II was redirected near it's end from a technical perspective with a focus on communications security technology to a "hands-on" perspective with a focus on Network Security Administration for both commercial and military Sensitive Unclassified environments. The NetWare Security Administrator's Security Guidance Handbook was the result of that redirection.

It was recognized that Government and commercial organizations face a common problem of having trained personnel rotate on to new assignments, leaving inadequately trained replacements to administer the networks. In addition, it was noted that many organizations which have NetWare Version 3 installed are contemplating the migration to Version 4, but their administrators have not been trained to manage NetWare Version 4 networks. The purpose of the Handbook was to provide specific security guidance for this group of administrators, including direction on where to find additional guidance on various security-related topics.

The importance of this redirection has been recognized and will be carried into Phase III with the development of a comprehensive set of network security administration tools. In addition, the scope will be broadened to include support of Microsoft Windows NT security administrators as well.

This Page Intentionally Left Blank

Section 1

Introduction

This Page Intentionally Left Blank

1.0 Introduction

This Final Report summarizes the results of a series of network security analyses performed by Secure Solutions under Phase II of the Small Business Innovation Research (SBIR) Program for the U.S. Navy's Space and Naval Warfare Systems Command (SPAWAR) under Contract Number N00039-93-C-0099, SBIR Topic Number N91-061, *"Placement of Network Security Services for Secure Data Exchange."*

The introduction describes the results of the Phase I effort and provides other background information on why this Phase II research effort was initiated, describes the scope, objectives, and approach used in the Phase II effort, and describes the organization of the report.

1.1 Background

Naval Command and Control, Communications and Computers, and Intelligence (C^4I) systems are hosted on shipboard, submarine, shore, airborne, and space platforms and must consequently operate in a variety of hostile environments. Diverse local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs), as well as client-server technologies and Network Operating Systems (NOSs), are used to support these C^4I systems. A major thrust is to interconnect these networks for the purpose of sharing information and improving the survivability of the overall network. To support application-level interoperability among C^4I systems which use these networks, the use of a layered architecture is imperative. Furthermore, with the current migration from centralized host environments to distributed client-server environments, it is imperative that a distributed approach to security be adopted.

Phase I of this SBIR effort focused on the Open Systems Interconnection Reference Model (OSI RM), the most well-known framework for a layered architecture. It is shown in **Figure 1-1** and described in the International Standards Organization (ISO) International Standard 7498 (ISO 7498). The Security Architecture for the OSI RM, described in ISO 7498-2, identifies five basic categories of services: *data confidentiality, data integrity, authentication, access control, and non-repudiation.*

The placement of security services and mechanisms within the OSI Reference Model has always been controversial because ISO 7498-2 limits the layers where they may be placed. For Layer 2, the Data Link Layer, it states that only data confidentiality may be provided. The IEEE 802.10 LAN/MAN Security Working Group is developing the Standard for Interoperable LAN/MAN Security (SILS). SILS includes a description of the Secure Data Exchange (SDE) protocol which operates within Layer 2 and supports data confidentiality, data integrity, authentication, and access control. Due to their efforts, ISO is considering modifying the OSI Reference Model to include these services at Layer 2, as shown in **Figure 1-2**.

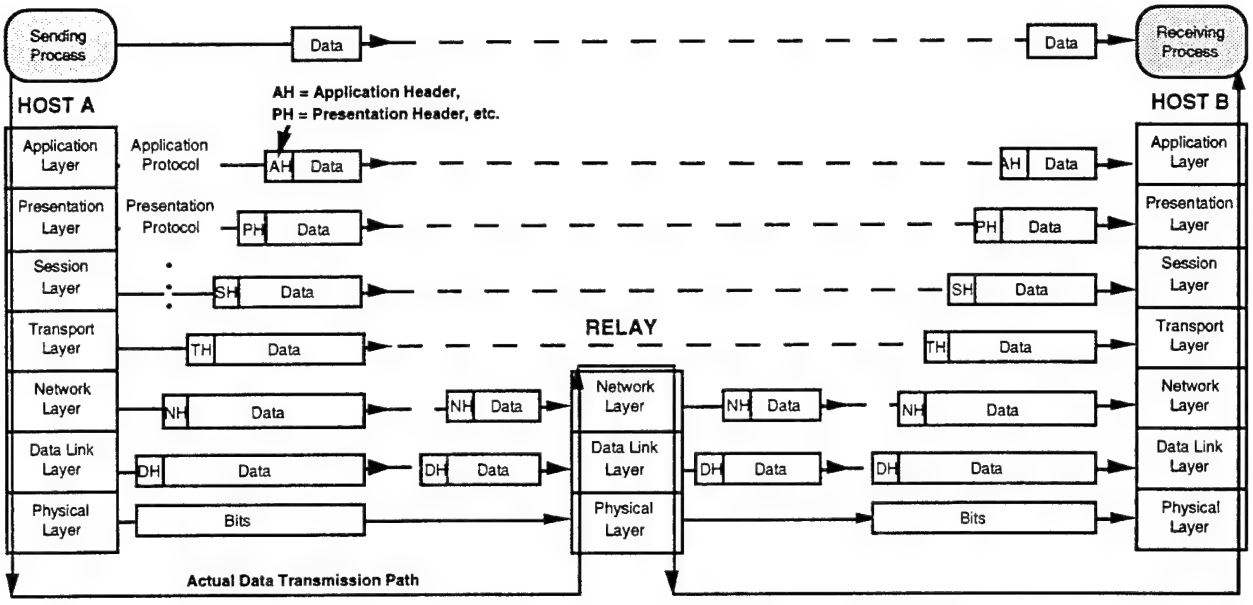

Figure 1-1. Layered Architecture of the OSI Reference Model

Service	Physical	Data Link	Network	Transport	Session	Presentation	Application
Data Confidentiality	●	●	●			●	
Data Integrity		S	●	●		●	
Authentication		S	●			●	●
Access Control		S	●	●			●
Non-repudiation						●	●

Legend:
● – ISO 7498-2
S – SILS

Figure 1-2. Allocation of Security Services to OSI Layers

Simply resolving the differences between standards organizations will still not lead to an optimal placement of security services among layers for the Navy. Optimal placement for the Navy will only be achieved if the placement of services are primarily driven by DoD information security (INFOSEC) assurance requirements and the greater constraints encountered in the Naval tactical environment. In this regard, it is critical that service placement selections be made in a manner that conserves bandwidth, supports real-time transmission requirements, and promotes survivability. For these reasons, the Phase I effort was undertaken to perform a thorough analysis to identify the security services that should be provided in each of the seven layers of the OSI Reference Model for Naval applications.

The Phase I effort produced the following accomplishments:

- The general services and functions were described for each OSI layer
- The security services and mechanisms to be allocated to the various OSI layers were defined
- Evaluation factors for analyzing placement options were defined
- Security services were allocated to the OSI layers using the evaluation factors.

The following conclusions were reached as part of the Phase I effort:

- There is a need for LAN security products (e.g., local and remote bridges) implementing security services and mechanisms at Layer 2 of the OSI Reference Model. These would support Naval mission-specific requirements for delivery/ response times
- The U.S. Navy needs to continue to support national and international standards development activities to ensure that Navy mission-specific requirements are taken into account as part of these efforts
- Both Type 1 and Type 2 security products are needed to support Naval missions. The following security products are needed:
  - Secure local bridge
  - Secure remote bridge
  - Secure LAN front end
  - LAN Security cards.

1.2 Phase II Scope

Phase II was intended to extend the work of the Phase I effort by performing demonstrations, conducting relevant follow-on systems engineering efforts, and holding meetings with vendors to stimulate interest in the development of LAN security products to support mission-critical Naval applications. The original Phase II contract involved the following work efforts:

- Task 1 – Demonstration of Phase I Concept
- Task 2 – Navy Security Standards and Applications Analysis
- Task 3 – Analysis of End-to-End Encryption and Traffic Flow Confidentiality
- Task 4 – Naval Network Security Requirements Analysis
- Task 5 – LAN Security Product Specifications
- Task 6 – Provide Briefings for Phase III Support
- Task 7 – Participate in Security Groups.

The Phase II effort began with a focus on documenting emerging communications security technologies from a technical perspective rather than from a "hands-on" Network Security Administrator's perspective. As Phase II progressed, it was recognized that new client-server technologies and NOSs introduced viable options for placement of security services and mechanisms. Participation in Security Groups, Task 7, included participation in Internet Engineering Task Force (IETF) security working groups. Through this task and others, it was noted that with the rapid expansion of networking technologies, user connectivity demands, and security administrator options, Navy and commercial network security administrators needed well defined recommendations on what security features to activate and what additional security mechanisms (e.g., firewalls) to implement in their specific Naval environments.

In response to these changing needs of the Navy, Secure Solutions, Inc. redirected the Phase II work effort. Tasks 1, 2, 3, 4, and 7 had already been completed prior to the redirection. Tasks 5 and 6 were canceled and replaced with a new Task 5:

- Task 5 (redirection) – NetWare Administrator's Security Guidance Handbook.

1.3 Phase II Objectives

The technical objectives for Phase II, including consideration for the redirection of Task 5, were to:

- Determine quantitatively if the implementation of security protocols at lower OSI layers in relays (or front ends) will significantly reduce delivery time across a LAN internetwork

- Consider what security functions and services should be standardized to support network applications, assess which security services should be allocated to the communications protocol stack, review the status of standardization in both commercial and Government sectors, and report the findings and provide guidance to system designers concerning identification of security mechanisms that implement the security services, placement of those mechanisms, and implementation of the security standards

- Determine the extent of potential traffic flow information leakage due to the use of protocol control information that is not encapsulated when end-to-end encryption is used, and discuss the merits of the solutions to counter those vulnerabilities

- Identify the high-level security implementation requirements for Navy networks so that future studies can focus on the strengths and deficiencies of security products and identify areas where additional security products are needed

- Provide consolidated, concise, and easy to read security guidance on Novell NetWare to acquaint management and new network administrators with all major security issues and provide pointers to more in-depth documentation on each subject so they will be able to take the correct steps to counter any threats that may arise

- Participate in Navy, U.S. Government, and International working groups to develop recommendations for selecting security services in Navy systems, with an emphasis on the Navy Integrated C^4I Security Architecture.

1.4 Phase II Approach

This study was accomplished by performing the following tasks:

- *Demonstration of Phase I Concept* – Work with Naval Command, Control, and Ocean Surveillance Center's RDT&E Division (NRaD), Naval Research Laboratory (NRL), and Naval Surface Warfare Center (NSWC) to define a network configuration for evaluating delivery time, develop a mathematical model for computing delivery time, and search for relevant sources to provide a demonstration of security services most suited to Navy systems

- *Security Standardization* – Review recent security-related studies and Naval computer and telecommunications architectures contemplated for the future in order to understand the specific needs of the Navy, and interview members of standards bodies and review standards to assess their progress and to consider whether the required security services and functions have been provided

- *Traffic Flow Confidentiality* – Analyze end-to-end encryption (E^3) and traffic flow confidentiality options and recommend options to enhance security in various environments

- *Requirements Analysis* – Conduct requirements definition and systems engineering studies of the DoD Goal Security Architecture (DGSA), Multilevel Information Systems Security Initiative (MISSI), and Integrated C^4I Architecture to define Navy mission-specific needs for network security

- *NetWare Security Guidance* – Review Novell NetWare security features and deficiencies, assess their impact on commercial and Navy Type 2 (Sensitive Unclassified) processing environments, review related third-party support products, and report the findings in a NetWare Administrator's Security Guidance Handbook

- *Security Working Groups* – Participate in security working groups, including the American National Standards Institute Accredited Standards Committee for Open Systems Security (Task Group X3T5.7), IEEE Security Working Group for Standard Interoperable LAN/MAN Security (IEEE 802.10), and the Internet Engineering Task Force Security Area working groups.

1.5 Report Organization

The main body of the report is organized as follows:

- **Section 1** – Introduction

- **Section 2** – Summary and Conclusions of Phase II Effort

- **Section 3** – Proposed Direction for Future Work Efforts

The following appendices are provided to supplement the main body:

- **Appendix A** – Acronyms

- **Appendix B** – References.

Section 2

Summary and Conclusions of Phase II Effort

This Page Intentionally Left Blank

2.0 Summary and Conclusions of Phase II Effort

Phase II consisted of six tasks, as discussed in Section 1. The first four tasks resulted in technical reports, the fifth task resulted in a security handbook, and the last task (Task 7) resulted in a series of trip reports on the security working group meetings attended. Discussions of the background, conclusions, and recommendations for each task are provided in the following paragraphs.

2.1 Task 1: Demonstration of Phase I Concept

The Phase I effort made the qualitative observation that the delivery time through a secure relay (or secure front end) could be improved (reduced) if the security protocol is implemented at a lower layer within these components. Task 1 of the Phase II effort demonstrated quantitatively how much delivery times can be improved (reduced) by implementing security protocols at lower OSI layers in relays (or front ends). The approach described three variations of an internetwork model consisting of two 802.3 LANs interconnected through a backbone Fiber Distributed Data Interface (FDDI) LAN. The variations involved three different types of secure relays – bridges, routers, and transport protocol converters – which interconnect the 802.3 LANs with the FDDI LAN. Each relay uses different types of security protocols at different OSI layers: the Secure Data Exchange (SDE) protocol at Layer 2; Security Protocol 3 (SP3) or the Network Layer Security Protocol (NLSP) at Layer 3; and Security Protocol 4 (SP4) or the Transport Layer Security Protocol (TLSP) at Layer 4.

Conclusions regarding the impact on host-to-host delivery time as a function of where security protocols are placed within OSI layers were as follows:

- Latency is a function of distance between sender and receiver and the number of protocol stacks that must be traversed. It is also a function of the amount of time needed to access a shared service. Latency in the intermediate nodes is a function of how high in the protocol stack the data must go before it goes back down

- Providing end-to-end security services, as opposed to link security services, improves (reduces) delivery time because security encapsulation and decapsulation functions are only performed at the source and destination host. When link security services are used, security encapsulation and decapsulation functions are performed repeatedly, thereby increasing the host-to-host delivery time for a given network configuration

- If security services are used in the intermediate nodes, there will be additional latency due to security processing in both halves of each intermediate node stack. If the security processing has to be in a layer higher than the intermediate node would otherwise use to perform its normal functions, then additional latency is added due to having to process higher layers in the intermediate nodes' stacks

- Intermediate node security services are not needed for end-to-end data security, but are needed for traffic flow security when it is implemented in the lower layers.

The following recommendation was made from the standpoint of delivery time evaluation:

- Whenever possible, the Navy should provide end-to-end security services by implementing security protocols within hosts at the top of layer three or higher. This will minimize the host-to-host delivery time in comparison with providing link security services.

Task 1 identified potential sources which can be used to qualitatively determine the improvement in delivery time through the three variations of a LAN internetworks.

2.2 Task 2: Navy Security Standards and Applications Analysis

It is through standards that the computer and communications industry can achieve the goal of interoperability, and it is through security standards that can this goal can be met in a secure manner. To better understand why security standards are needed in supporting the development of secure computer and network systems, and the types of standards that are needed, Task 2 produced the following accomplishments:

- Reviewed recent security studies on distributed processing and military telecommunications architectures in order to determine what security functions and services should be standardized to support computer network applications

- Reviewed security guidance documents and standards and determined the status of those standards

- Described security mechanisms that can be implemented to provide the security services specified by the standards. The services include authentication, access control, audit and accountability, confidentiality, integrity, non-repudiation, and service assurance. The mechanisms include peer address checking, challenge-response exchanges, certification authorities, discretionary and mandatory access controls, digital signatures, notary services, encipherment, traffic padding, integrity check values, sequence numbering, timestamps, and redundancy

- Suggested additional factors concerning the choice and placement of network security mechanisms that must be considered when evaluating architectural alternatives for secure computer and communications systems.

The following conclusions were reached as part of the Task 2 effort:

- **Technological Advances** – Networking is evolving faster than any other area of automation. As a result, an insatiable demand for even greater capabilities has developed. Developers have responded with more powerful, more reliable, and more secure communications technologies and products. Improvements include:

- *Bandwidth* – Fiber optic media has emerged as the technology of the future, because it can support broad bandwidths at reasonable costs. FDDI incorporates dual counter-rotating fiber optic rings to provide high bandwidth for local area network communications. The Distributed Queue Dual Bus (DQDB) subnetwork of a metropolitan area network incorporates dual fiber optic rings to provide the Switched Multi-megabit Data Service (SMDS). The Broadband Integrated Services Digital Network (B-ISDN) incorporates cell-relay-based Asynchronous Transfer Mode (ATM) and Synchronous Optical Network (SONET) to provide high-performance multimedia wide area network communications

- *Multimedia* – Network providers are combining telephony, cable broadcasting, and digital transmissions. Multimedia capabilities will change the way the Navy accomplishes its missions. Multimedia is identified as the basis for the Command Global Information Exchange System (GLOBIXS) network of the Integrated C^4I Architecture. Interactive video applications and video conferencing are expected to become common activities

- *Enterprise hubs* – Enterprise hubs introduce switched buses which offer significant speed and security benefits that cannot be realized on the traditional contention-based broadcast LAN

- *Wireless LAN* – This technology is evolving due to the success of the portable computer and the cellular telephone. Demand has created a market and that market is motivating developers. Wireless LANs will provide flexibility for Government agencies, but pose new challenges with respect to security

- *Multilevel Security* – From a security perspective for the military, the most important development efforts are in the area of multilevel processing. Standards bodies and system developers are well aware of the need to label subjects and objects and to base access control decisions on those labels. Automation will someday (probably no less than 10 years) be capable of allowing cleared and uncleared users to share the same resources across multilevel networks. The user community would have more freedom to operate automated systems in less secure environments since they would be assured that the computers and networks can provide the necessary security.

- **Status of Standards** – Security standards for most areas are relatively new, though there is a significant commitment within industry and government toward developing and implementing standards. Most security standards have not yet been widely implemented, and are therefore not stable. Vendors hesitate to implement products based on draft standards. Even when standards are finalized, they are not stable. Stability comes when the standards have been implemented and there is little technological pressure to change them. Since many of the international standards are not stable, existing standards that are more widely implemented may be used in the interim.

- **Naval Environment** – Studies concerning the architecture and security implications for four Naval systems were reviewed. They were:
  - Battle Management Command and Control System
  - Submarine Command System
  - Integrated Interior Communications and Control $(IC)^2$
  - Integrated C^4I (formerly Copernicus) and supporting communications systems.

  Required security services were identified and generally found to conformed to those that apply to all networked or distributed systems. Furthermore, the specific mechanisms that are required for the Navy systems are those that are commonly used. **Figure 2-1** summarizes the security services and mechanisms suggested in the various studies and also indicates that standardization efforts have addressed provisions for all of the identified services and mechanisms.

	Services									Security Mechanisms															
Security Requirements	Identification and Authentication	Confidentiality	Integrity	Access Control	Non-Repudiation	Service Assurance (Availability)	Discretionary Access Mechanisms	Mandatory Access Mechanisms	Labelling	Integrity Check Value	Audit and Accountability	Object Reuse	Trusted Path	Encryption	Key Management	Network and Security Management	One-Way Hash Algorithm	Digital Signatures	Certification Authorities	Challenge-Response Protocol	Sequence Numbers	Timestamping	Redundancy	Selective Routing
MCCR INFOSEC Study	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Distributed Systems Security	•	•	•	•	•	•	•	•	•	•				•			•	•	•	•	•	•	•	•	•
JMCIS Study																									
Standard Navy Shipboard LAN																									
Battle Management System	•	•	•	•	•	•	•	•	•	•	•			•		•									
Submarine Combat System	•	•	•	•	•	•	•	•	•	•	•			•		•									
Integrated C4I Security	•	•	•	•	•	•	•	•	•	•	•			•	•	•									
Provided by Standards	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Figure 2-1. Required vs. Provided Security Services and Mechanisms

- **Security Mechanisms** – Network security mechanisms are categorized according to the following security services, as shown in **Figure 2-2**:
  - Authentication
  - Access Control
  - Audit and Accountability
  - Confidentiality
  - Integrity
  - Non-Repudiation
  - Service Assurance.

Authentication

- Peer Address Checking
- Authentication Exchange
  - Passwords
  - Supporting Devices
    - Hand-held devices
    - Smart cards
    - Biometric readers
  - Challenge-Response
    - Symmetric Encipherment
    - Asymmetric Encipherment
- Certification Authority
- Continuity of Authentication

Confidentiality

- Physical Protection
  - Isolation
  - Selective Routing
- Information Hiding
  - Symmetric Encipherment
  - Asymmetric Encipherment
  - Traffic Padding
- Partial Accessibility
  - Internal Fragmentation
  - Data Scattering

Access Control

- System-Oriented Access Control
  - Object Reuse
  - Trusted Path
  - Connection Timeout
- Discretionary Access Control
  - Access Control Lists
  - Capabilities
  - Authentication Server
- Mandatory Access Control
  - Security Labels
  - Routing Control

Integrity

- Error Detection
  - Error Detection Codes
  - Integrity Check Values (ICV)
  - Message Digests
- Encryption for Integrity
  - Cryptographic Seal
  - Digital Signature
- Sequence Protection
  - Sequence Numbers
  - Cryptographic Chaining
  - Timestamps
  - Reflection Bits
  - Source Addresses

Audit and Accountability

- Audit Mechanism
- Alarm Mechanism

Service Assurance

- Redundant Components
- Fault Tolerance
- Priority Processing

Non-Repudiation

- Digital Signature
- Notary Service

Figure 2-2. Generic Security Mechanisms

2.3 Task 3: Analysis of End-to-End Encryption and Traffic Flow Confidentiality

The use of end-to-end encryption (E^3) services in internetworks where the trustworthiness of intermediate subnetworks is not provided is a critical capability for the Navy. The data to be transferred from the source host to the destination host can be encrypted at the source and not be decrypted until it reaches the destination. Advantages of using end-to-end encryption in internetworks could include the flexibility to connect classified hosts to commercial networks. Even if the data traverses subnetworks or components that are not trustworthy, the data still retains its assurance of confidentiality so long as the encryption keys are not compromised and the encryption algorithm is sufficient to preclude a cryptanalytic attack.

Although end-to-end encryption protects the user data from observation, it does not safeguard against traffic flow leakage from protocol headers that are applied after the end-to-end encryption is performed. Security-relevant information that may be available in the headers or derived from the headers includes source and destination addresses, priorities, security labels, message lengths, transmission frequencies, sequence numbers, flow control information, message routing lists, lifetime of the *protocol data unit* (PDUs), and checksums. It is necessary to determine the extent of the vulnerabilities associated with sending headers in the clear in order to eliminate or reduce the traffic flow confidentiality problem. The nature of this information provides a basis for determining the advantages and disadvantages of providing traffic flow confidentiality services at the lower layers after the headers have been applied.

Task 3 analyzed protocol control information (PCI) associated with LAN and WAN communication protocols and assessed what information can be derived from the protocol headers through traffic analysis, which is the inference of information from observation of traffic flows (e.g., their presence, absence, amount, direction, route, frequency, time of transfer, length, and other security-relevant information).

The report described the utility of traffic flow confidentiality options that may be employed to reduce the risk of exposure to traffic analysis. The primary measure to implement traffic flow confidentiality is the prevention of direct observation of information. This is accomplished with a confidentiality service, i.e., through the use of encryption for most networks or a protected distribution system for some links of a network. In addition, the ability for an adversarial traffic analyst to derive information must be prevented. This is accomplished through the insertion of dummy traffic, data padding, route control, data unit segmentation, address hiding, and timing techniques. The padding mechanisms must be implemented before the confidentiality mechanisms in order to be effective.

The major conclusions of Task 3 were:

- In most environments, the implementation of traffic flow confidentiality is unwarranted due to the processing overhead associated with its use
- In those cases where traffic flow confidentiality is warranted, it may be advisable to implement a combination of mechanisms at different layers. The OSI Security Architecture, ISO 7498-2, identifies the layers at which traffic flow confidentiality can be provided: the Application Layer, Network Layer, and Physical Layer
- Implementation of traffic flow confidentiality at the Application Layer will allow the user to be selective. In addition, this provides end-to-end (user-to-user) service. By implementing traffic flow confidentiality at a lower layer, traffic flows for the End System as a whole can be masked
- Data padding performed at the Application Layer is the first step in effectively concealing message sizes and types. Data padding can also be accomplished at the Transport, Network, and Data Link Layers, perhaps with less impact because it would not be applied to individual applications. NLSP is the only protocol that is specifically designed to perform data padding for traffic flow confidentiality
- When padding is accomplished at the Application Layer, encipherment will be accomplished at the Presentation Layer after context translation. When padding is accomplished at the Network Layer, encipherment can be accomplished immediately after by the same protocol entity
- SDE can be used at the Data Link Layer to encapsulate Connectionless Network Protocol (CLNP) and Logical Link Control (LLC) headers on LANs. Although ISO 7498-2 does not call for traffic flow confidentiality services at the Data Link Layer, SDE can provide limited traffic flow confidentiality within a LAN, or across multiple LANs connected by remote bridges. What remains exposed to observation by other nodes on the LAN are the Media Access Control (MAC) addresses, and time and frequency of transmission. Since SDE cannot be implemented with WAN protocols, X.25 and Link Access Procedures–B (LAPB) headers expose information that can only be protected at the Physical Layer
- Traffic padding can generate dummy traffic between two End Systems or any segment of a network to help camouflage heavy traffic loads. While traffic padding is an important traffic flow confidentiality mechanism, it incurs much overhead because connections must be padded to near capacity in order to conceal when peak traffic actually exists
- Segmentation with encryption conceals the original size of data units formed by application processes. Segmentation is performed by some Application Layer protocols, Transport Protocol Classes 4 (TP4) and 1 (TP1), NLSP, CLNP, X.25, and SDE

- Timing techniques to delay low priority messages can be employed when there is heavy traffic so the load appears to stay at an even level

- Route control, provided by CLNP, is an effective support mechanism to help ensure that traffic is not routed over insecure subnetworks or components. It can also be used to disperse PDUs and PDU segments over diverse paths. However, traffic analysts may still be able to infer when there is a high volume of traffic between two particular hosts if addresses or PDU types can be identified, even though they cannot observe the full load. Route control requires the use of additional fields in the PDU to explicitly identify the path to be traversed. If a security protocol is used to encapsulate the CLNP header, an additional CLNP protocol header may be needed below the security protocol to implement route control over the untrusted portion of the internetwork. For these reasons, there is significant overhead associated with route control. Routing control also introduces security risks which may outweigh the benefits of its use

- CLNP headers contain information that a traffic analysts can use to recognize when particular activities are underway at the source and destination organizations. Therefore, it is preferable to implement NLSP or SP3 below CLNP in environments where the security protocol peer entities are End Systems so the actual addressee can be hidden

- Another reason for implementing NLSP or SP3 below CLNP is that CLNP has a lifetime field (i.e., expiration counter) in the header that is decremented by each Intermediate System and used to eliminate expired PDUs from the network. An adversary could modify the lifetime field in order to flood a network or to cause messages to expire before they arrive at their destination and still maintain the normal traffic flow out of the adversarial station

- FDDI can be protected by physical means or through full period encryption on each point-to-point link

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) can be partially protected with full period encryption, but the preamble and starting delimiter must be sent in the clear to achieve bit and frame synchronization

- Full traffic flow confidentiality can only be provided at the Physical Layer in certain circumstances: two-way simultaneous (full-duplex), synchronous, point-to-point transmission. Full traffic flow confidentiality is not effective against active threats unless integrity mechanisms are also utilized in a cooperative manner

- A mechanism that offers a high degree of protection from wiretapping of the link between two remote bridges which are in close proximity is a Protected Distribution System (PDS). However, a PDS would not protect traffic from observation by other stations on a LAN. Full period encryption provides a similar service when the remote bridges are geographically remote.

The recommendations of the Task 3 study were:

- Implement traffic flow confidentiality mechanisms only when absolutely necessary because they require significant overhead and may cause network congestion
- Consider implementation of a combination of mechanisms at different layers
- When traffic flow confidentiality is deemed necessary, the protocol stack should primarily include traffic flow confidentiality at the Network Layer for internetwork traffic, and at the Data Link Layer, when possible, for traffic contained within the LAN
- Traffic flow confidentiality on a link basis should be more widely implemented for the links that connect End Systems to an internetwork. This can be implemented most robustly using full period encryption. An alternative that is feasible for some sites is to use physical security measures such as a PDS
- Avoid the use of route control for traffic flow confidentiality due to excessive overhead associated with its use, the need for two CLNP headers when a security protocol is applied below the upper CLNP header, and security risks that accompany its use
- When deciding whether to implement confidentiality services at the Network or Data Link Layers, system architects must consider what type of network is involved. In a WAN, subnetworks and routing are implemented at the Network Layer. Similar subnetwork and routing functions are exhibited at the Data Link Layer in LANs. For these reasons, the following layer placement options for traffic flow confidentiality are recommended:
  - **Application Layer** – Application Layer traffic padding mechanisms should be reserved for those sites or applications that are determined to have traffic profiles which can be used to infer classified missions or information. When an application processes classified information that is highly desired by an adversary and that information is transmitted over an internetwork where the adversary may have an opportunity to observe, modify, or delay the information, a data padding mechanism should be placed in the Application Layer to disguise the message type and size. Timing techniques should be implemented in the application process to delay low priority traffic during peak traffic periods and dummy traffic should be generated during low traffic load periods so that high loads cannot be identified
  - **Presentation Layer** – end-to-end encryption should be applied in conjunction with the traffic padding mechanism in the Application Layer

- **Network Layer** – Network Layer mechanisms can be applied to traffic originating from a broad range of applications on the host and are less costly to implement than if they were implemented in each application process or protocol. If a single Application Service Element (ASE) or operating system utility is used to protect all application processes, then implementation costs will be comparable. Data padding, end-to-end encryption, and the generation of dummy traffic should be performed at the Network Layer for most environments, particularly when it is necessary to camouflage all traffic between two hosts or a set of hosts. The use of dummy traffic at the Network Layer should be limited to hosts that require strong traffic flow confidentiality so that the network does not become overly congested. In most cases, it would be better to generate dummy traffic at the Data Link Layer for dedicated links between two stations

  Additional protocol options that could be implemented at the Network Layer include segmentation, disbursement of the segments, and route control. Route control can only be implemented at the Network Layer. These mechanisms have much less impact on network performance than does the generation of dummy traffic and should be used when portions of the network are outside the controlled environment

- **Data Link Layer** – The generation of dummy traffic across the link between a DTE and a DCE should be used to hide the true traffic load to and from the End System without causing congestion on the network. Timing techniques should be implemented on the same links as well, and for the same reasons

  The segmentation, data padding, and encapsulation capabilities of SDE can be used on LANs to hide PCI from other stations that are authorized to connect to the LAN when pairwise unique keys are employed between stations. SDE is also effective between multiple LANs connected by local or remote bridges and can be used to provide end-to-end encapsulation within a LAN internetwork

- **Physical Layer** – Full period encryption should be used to protect individual point-to-point links. In particular, full period encryption should be used on links between remote bridges that are outside of protected enclosures and protected paths

- **Physical Installation** – A protected distribution system should be installed to protect cables that traverse areas that are not protected at the level of the data being carried on the network. For example, if two shipboard LANs are installed in areas of a ship that are not adjacent, the cable connecting the remote bridges should be protected by a PDS.

2.4 Task 4: Naval Network Security Requirements Analysis

Task 4 analyzed the DoD Goal Security Architecture (DGSA), Multilevel Information Systems Security Initiative (MISSI), and Navy Integrated Command and Control, Communications and Computers, and Intelligence (Integrated C^4I) programs in order to determine security implementation requirements for Navy networks in light of emerging technologies. The study identified 10 major security implementation requirements. They are to provide security for the following:

- Open systems architecture
- Interconnectivity and distributed processing
- Use of COTS / GOTS hardware and software
- Processing at extremely high speeds
- Multilevel security
- User mobility
- Multimedia communications
- Firewalls
- Selectable security services
- Multicast routing.

The analysis included a brief review of the current environment, characterized by existing and proposed network security products, and discussed possible deficiencies which may require the development of additional security products. These findings were preliminary and merit further investigation.

The major conclusions of the Task 4 study were that it appeared there were not adequate security products to meet the requirements for:

- **Secure User Mobility** – As networks become more robust and users become more mobile, users will demand access to their data from any station in the network. As computers become more portable, they will at times require broadcast media for connectivity to the network rather than cables. Likewise, when a computer is carried around a ship, aircraft, hospital, or other workplace, the connection must not be lost or interfered with, and must not interfere with other signals such as radar and navigation. Technology is beginning to address the need for mobility, but security has not been a driving force in the development efforts

- **Secure Multimedia** – Some trusted workstations are able to apply two types of sensitivity labels to the information they represent, one that indicates the classification range for the user and one that indicates the sensitivity of a particular window. The label for the information will be at the same or lower sensitivity level as the user's session label. Network security mechanisms also indicate a workstations range of permissible classifications and the classification level for a particular session, but no single protocol has been designed to handle both. Multimedia communications will require such labeling. There are other security issues that pertain to multimedia. In particular, as multimedia applications are introduced to run at the speeds of ATM, the minimum acceptable transmission speeds will rise rapidly. Security mechanisms must be developed to support these speeds. Some SONET and ATM encryptors are being developed, but encryptor products are needed at higher layers as well

- **Secure Firewalls** – The security community is not in agreement as to whether firewalls are beneficial or detrimental. Some argue that firewalls provide a false sense of security. Since, by definition, some protocols must be permitted to pass traffic through the firewall, that traffic can be dangerous and difficult to protect. Others argue that firewalls can filter out specific types of communications that are known to be high risk. Regardless, firewalls are not currently very effective. Since it is not presently possible to install adequate security in every user workstation and server, and since interconnectivity is needed for operational purposes, there is presently an urgent need for secure firewalls

- **Secure Multicast Routing** – In order to minimize network congestion, multicast techniques are being developed to send one copy of a message across parts of the network and then have routers burst the message into multiple copies for delivery to all intended recipients. This capability is imperative as multimedia applications become more common. This capability is also imperative as communication bandwidths to and from mobile platforms (e.g., ships) are always less than desired. As multicast protocols are developed, security issues must be addressed to ensure that routers correctly deliver traffic to all intended users and at the same time do not deliver traffic where it is not intended. Other security implications concern the application of security protocols that encrypt the destination address in a protected header. Since the multicast protocol must be able to modify the address entries, it may conflict with the use of an end-to-end security protocol.

Since the technologies and standards that support mobile users and multicast capabilities are not stable, Task 4 suggested that it may be premature to attempt to develop security products for these areas. *(Note: since the Task 4 report was published, much progress has occurred in these areas.)* However, participation in the standardization efforts by security engineers was highly recommended in the Task 4 report. It also stated that security products should be developed to meet near-term requirements for the following:

- **Secure Multimedia –** Multimedia applications are being developed and will soon be in wide use on internetworks. Existing mechanisms that provide security services are not suitable for the wide bandwidth of multimedia, or for providing unique security such as supporting multiple sensitivity labels for video and whiteboard windows. Whiteboard windowing is a service that generally piggybacks on video teleconferencing to provide a second window that displays the speaker's presentation slides. The audience can then simultaneously view the speaker and the slides. An advantage of whiteboarding is that it uses a narrow bandwidth to provide the service

- **Secure Firewalls –** Several types of firewalls are urgently needed. Perhaps the most important are Network Layer firewalls (routers). However, there are also requirements for Data Link Layer firewalls (bridges) and for application specific firewalls (Application Gateways) that can be installed in-line with the current generation of Network Layer firewalls.

Further studies are needed to assess these areas that appear to be deficient. Additional products are needed to meet the security needs in these two areas. When user mobility and multicast technologies are more stable, security protocols, products, and interfaces will be needed in those areas.

2.5 Task 5: NetWare 4 Administrator's Security Guidance Handbook

A decade ago, centralized multi-user mainframe computers were the standard architecture for allowing users to share software applications, files, printers, and other resources. The advantages of the centralized architecture were that it allowed the sharing of data and expensive resources and provided for central control and management of the data. The disadvantages were that it was not flexible in meeting user needs and did not encourage creativity in the use of data. In addition, it was a single point of failure.

The introduction of PCs brought flexibility in the way users could manipulate their data, and also encouraged the proliferation of distributed sources of data. This often meant no central control of the information and, furthermore, it meant conflicting sources of information. In addition, it meant higher equipment costs because each user wanted a printer attached to their PC so they would not have to carry a diskette to another PC in order to print a file. Very quickly, the LAN became popular as a tool to enable information, software, and printer sharing similar to what users experienced with the centralized architecture. The LAN combined the flexibility of desktop PCs with the sharing capabilities of the centralized processor.

Dedicated servers soon emerged because some server functions, such as database management, required more power than a non-dedicated PC could provide. As depicted in **Figure 2-3**, many functions have been migrated to dedicated servers. For example, dedicated servers are used to support not only application files,

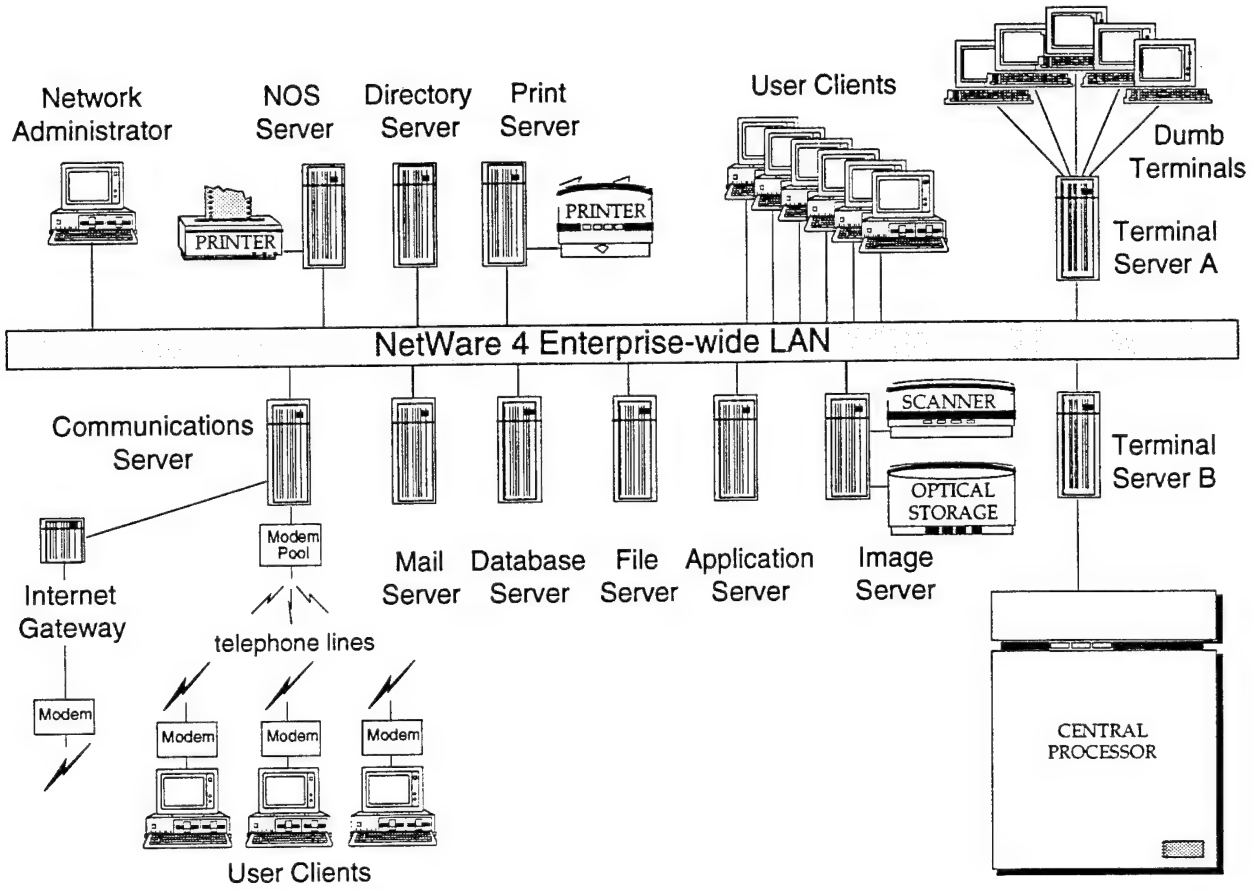

Figure 2-3. A Robust Client-Server Environment

databases, and print spooling, but also central LAN management and security, fax machines, graphic scanning, mailboxes, dial-up modems, and directory services. Even dumb terminals can still access a centralized host connected to the LAN through the use of terminal servers. Client-server strategies create relatively inexpensive computing platforms that are easy to customize for specific applications and provide magnitudes more processing power than the centralized systems they replace. In addition, they are scalable to meet current and future Naval needs.

With the centralized host model, management and security were relatively straightforward. Today, placing files and databases on dedicated servers has several of the advantages that were present in centralized systems: the centralization of data management facilitates the supervision and control of information; the servers are easier to secure and maintain because they are in one location managed by one authority; and backups are simplified for the same reasons. In fact, with fult tolerance and redundancy features, LANs can often provide a higher level of service assurance than can a mainframe. Fault tolerance and recovery capabilities are designed into many networks in order to minimize the risk of the network being unavailable and to maximize the speed of recovery when it is unavailable.

Approximately 60 percent of the network operating systems (NOSs) in operation today are Novell NetWare. Other major NOSs include AppleShare, Banyan's Vines, Artisoft's LANtastic, and Microsoft's recently introduced Windows NT. Novell NetWare was the first true file-server system available for PC LANs. NetWare runs on most PCs in either a DOS or Windows environment and supports DOS, OS/2, and Macintosh workstations. A NetWare file server makes it possible for programs running on user workstations to locate and retrieve files from the server just as though the files were being retrieved from the workstation's local hard disk. To the application program, the files look and act just as they would if they were stored locally. Applications can also be located on NetWare servers for transparent access from workstations.

NetWare 3 is currently the most widely installed version of NetWare. The management database for NetWare 3, called the *Bindery,* is specific to one server; that is, this version is designed to operate on single dedicated servers. Each NetWare 3 server is managed individually because there is no management communication between servers. Thus, the NetWare Administrator has to establish access rules in the Bindery of each NetWare 3 server. Two objects (e.g., users, printers) cannot be assigned the same name because they would not be distinguishable.

Novell's most current version of NetWare is NetWare 4. With version 4, administrators view the network as a single entity – *an Enterprise Network* – rather than as a collection of individual servers, each needing individual management and control. With NetWare 4, references to objects include both the name and location. Thus, two users (or other objects) having the same name can exist on the network, or even on the same server. User accounts are set up once and are given appropriate access rights to any server on the network for which they are authorized. The NetWare 4 Administrator establishes access rules with one database for the entire network. This database is called *NetWare Directory Services (NDS).* Servers can be added or removed with minimal effort and access rules can be applied uniformly across the network.

Government and commercial organizations face a common problem of having trained personnel rotate on to new assignments, leaving inadequately trained replacements to administer the networks. In addition, many organizations that have NetWare 3 installed are in the process of, or are contemplating, migration to NetWare 4, but their administrators have not been trained to manage NetWare 4.X networks. NetWare 4 includes new features that experienced NetWare 3 Administrators may not be aware of.

Because NDS is complex, the administrator must take certain precautions in order to avoid unknowingly creating vulnerabilities in the security structure. In addition, there are many third-party products that can be installed to further enhance security in sensitive environments. Security issues concerning sensitive environments, NetWare 4 features, and supporting third-party products must be understood by first-time administrators as well as trained NetWare 3 administrators in order to make intelligent decisions.

The purpose of Task 5 was to develop a NetWare 4 Administrator's Security Guidance Handbook. The handbook was intended for the inexperienced administrator who may not have a technical background with NetWare. The objective of the handbook was to provide consolidated, concise, and easy to read security guidance on Novell NetWare 4 so that the administrator will be able to take the correct steps to counter any threats that may arise. All major security issues and topics were raised at a very high level to acquaint the new administrator with the issues. Pointers to detailed references were included for the reader who wishes to investigate specialized topics of interest to a deeper level.

NetWare 4 security involves controlling user logins, controlling access rights to the NDS Directory tree, and controlling access rights to the file system, including setting file attributes. The first of the two major layers of security is implemented in NDS; the other in the file system. NDS is a special-purpose database which administers the security of resources, services, and user accounts. In other words, it is a logical map that allows users to locate and access resources (i.e., *objects*) anywhere in the network. NetWare Administrators are responsible for maintaining this logical map. The file system consists of volumes contained on the servers. Each volume has its own directory structure (not to be confused with the NDS Directory tree). NDS and the file system, shown in **Figure 2-4**, are separate, though closely related. In addition, login controls are implemented when user accounts are activated. Of course, physical protection of servers and their consoles is always necessary, as is security of the printing services.

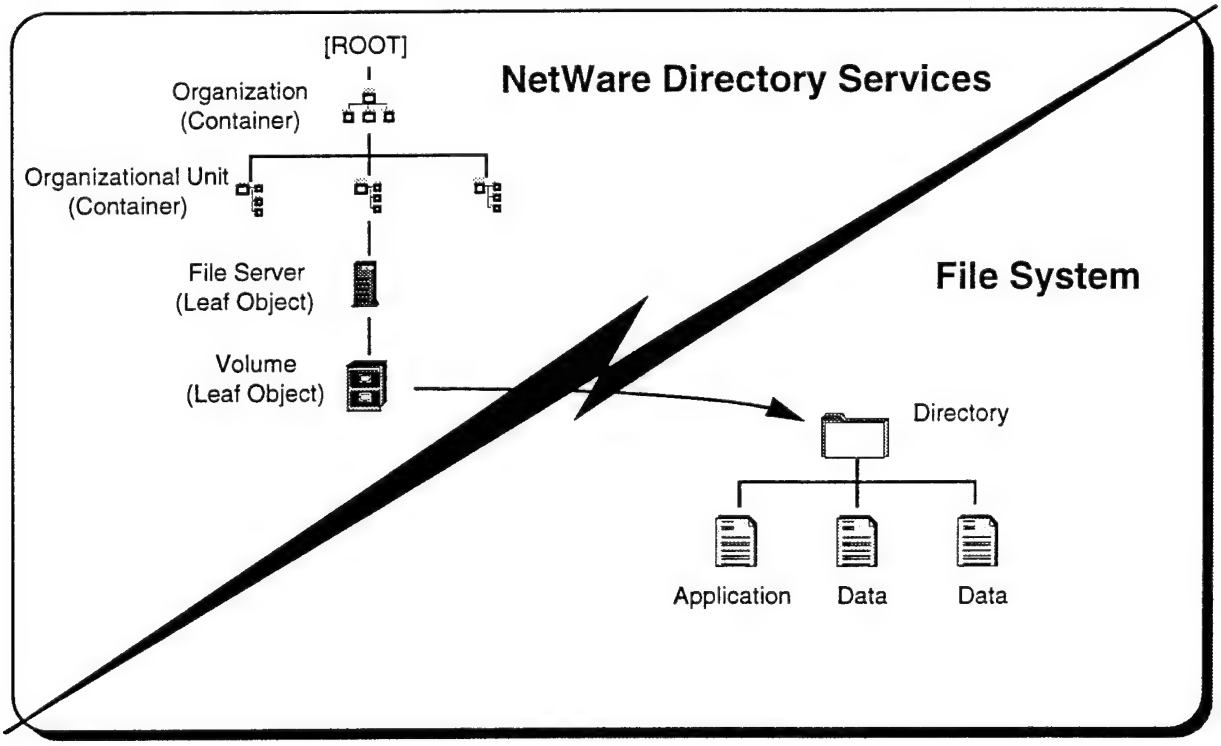

Figure 2-4. Relationship Between NDS and the File System

Security issues that are not solved by the implementation of NetWare 4 security features were discussed in the handbook. Third-party products that are available to help resolve some of those problems were identified. Other areas of interest include access controls for the workstation, enhanced authentication that incorporates one-time passwords, data encryption, network analysis and management, audit reduction, firewall security, and virus protection. Vendors have developed hardware and software products for each of these security areas. While most of the products discussed in the handbook operate independently of NetWare, they all function well in a NetWare environment. Some are designed as Virtual Loadable Modules (VLMs), which are executable files installed on the workstation, that load the DOS Requester software. The DOS Requester determines whether service requests should be directed to DOS on the local workstation or to NetWare on the server. A few are designed as NetWare Loadable Modules (NLMs) which are installed on servers to expand the functionality of the NetWare operating system. These are tightly coupled with the operating system and have instant access to other operating system services.

Naval LANs provide interconnectivity throughout a department or entire organization. This interconnectivity includes electronic mail and file transfers. Some organizations also extend the interconnectivity to other organizations. The Internet is an interconnected worldwide collection of networks that any organization may connect to if they choose. Navy organizations have recognized that it is to their advantage to allow their staff to connect to the Internet in order to extend the electronic mail and file transfers beyond their local organization. The NetWare administrator must be aware of the trend toward interconnectivity and take steps to support this need, while at the same time taking steps to protect the organization from outside tampering.

The NetWare 4 Administrator's Security Guidance Handbook described basic firewall architectures and discusses issues concerning external interfaces since many organizations are faced with the decision of whether to connect to external networks or remain isolated in the interest of better security. As discussed in NIST Special Publication 800-10 [NIST 94D], a *firewall* is needed to help protect the organization's LAN from unauthorized outside access. Another name for a firewall is *secure Internet gateway*. A firewall can be used to connect the organization's internal network to an external network and provide traffic routing services between the external and internal networks. It may also store information that the organization wishes to make public to the outside world (e.g., Web home pages and archives available for Anonymous FTP access). The traffic routing services may be implemented at the Network Layer by incorporating filtering rules in a router, or may be implemented at the Application Layer by using an Application Gateway. Each has advantages and disadvantages. Often the firewall will incorporate both approaches.

The NetWare 4 Administrator's Security Guidance Handbook attempted to surface security concerns that remain in spite of the installation of NetWare features and third-party products so that the security administrator could at least be aware of the concerns and be alert to changes that may elevate the importance of these issues.

The conclusions and recommendations of the NetWare 4 Administrator's Security Guidance Handbook were as follows:

- **Security Posture** – It is important that the security staff understand the threats and vulnerabilities of the system in order to reduce security risks to an acceptable level. This is accomplished through performance of a risk assessment. An important part of the risk assessment is the quantification of the sensitivity and criticality of the information to be protected. Decisions concerning the appropriate level of security to be implemented can only be made after determining the sensitivity and criticality of the data.

- **NetWare Administrator Training** – An overview of the NetWare NDS and File System structures was presented. While this will acquaint the administrator with the concepts, in-depth training on NetWare administration is required. This can be acquired from authorized Novell trainers, or when that is not possible, video training is available from several sources. Administrators should continue to attend NetWare training courses to broaden their exposure to aspects beyond basic administration. Personnel who will perform NetWare Auditor roles should also attend training courses. Participation in user groups is recommended to provide contacts among peers for the exchange of ideas and recommendations.

- **Implementation of NetWare Security Features** – The security administrator is responsible for enforcing the organization's security policy. Guidance concerning the implementation of NetWare security features was presented. Administrators should carefully review these recommendations and consider whether they are appropriate for their organization. They should also understand the concepts so that they can modify their implementations as necessary. Once the mechanisms have been activated, they should be tested and periodically retested. Even experienced administrators make errors. Tools are available to assist in the analysis. They can identify vulnerabilities that would not have been found had the tools not been used. Protocol analyzers and network management products should be mandatory elements of the administrator's toolkit.

- **Implementation of Secure External Interfaces** – Organizations that are considering installing modems for dial-up access or gateways to external networks face increased risks from many sources. These risks can be managed with the right tools. The handbook discussed some of the concerns and presented an overview of firewall technology. The criticality and sensitivity of the information must be well understood before a decision to permit dial-up access or connectivity to external networks can be made. Firewall technology has improved dramatically in the past year, yet there are those who still feel any firewall can be penetrated and a firewall only provides a false sense of security.

- **Use of Third-party Products** – NetWare was not designed to provide a high level of security. Accordingly, the security features of NetWare are limited. Third-party products are available to the administrator that has a need for them. The handbook discussed products that enhance workstation access controls,

provide stronger authentication than what is delivered with NetWare, provide data encryption for privacy, augment the administrator's analysis and management toolkit, implement firewalls of varying strengths, and provide virus protection. Many of these products are relatively inexpensive and are strongly recommended. Others are more costly, yet provide such strong degrees of security that they should be considered when the criticality or sensitivity of the data dictates.

- **Employee Security Awareness Training** – Any security program is doomed to fail if the user community is not educated, trained, and convinced of it's importance. Employee security awareness training that clearly describes the threat, purpose for the security policy, security policy, and user responsibilities is necessary in every organization.

2.6 Task 7: Participation in Security Groups

National and international working groups are developing security standards to promote interoperability and network security. The following working groups were selected for attendance in order to observe the progress of relevant standards and develop recommendations for selecting security services in Navy systems:

- Task Group X3T5.7 – Standards Committee for Open Systems Security (Accredited by American National Standards Institute) – meetings attended: August 1993
- Open Systems Environment (OSE) Implementors' Workshop (OIW) – National Institute of Standards and Technology (NIST) – meetings attended: September 1993
- IEEE 802.10 Working Group – Standard for Interoperable LAN and MAN Security (SILS) – meetings attended: November 1993, March 1994, and July 1994
- Internet Engineering Task Force (IETF) Security Area Working Groups – meetings attended: March 1994 and December 1994

In addition, meetings were attended at the National Security Agency to discuss the DGSA program, the Naval Research Laboratory to discuss Internet and Navy security programs, the Naval Computer and Telecommunications Station to discuss the Defense Message System, the Naval Air Force U.S. Pacific Fleet headquarters to tour the aircraft carrier USS Constellation, and the Naval Surface Force U.S. Pacific Fleet headquarters to tour the amphibious assault ship USS Essex. Participation in these meetings produced the following findings:

- **Task Group X3T5.7** – The Standards Committee for Open Systems Security was responsible for the development of three important international standards:

  – Security Frameworks for Open Systems (ISO/IEC 10181) – Security frameworks developed jointly as International Telecommunications Union (ITU-T) Recommendations and as a multipart International Standard, define the means of providing protection for systems, objects within systems, and interactions between systems. This includes databases, distributed applications, open distributed processing, and open systems interconnection. Frameworks define basic security concepts, possible classes of mechanisms, services for those classes of mechanisms, functional requirements of protocols, and general management requirements.

  Security frameworks are not concerned with specific implementations or methodologies for mechanisms. Other standards can use frameworks by incorporating concepts and providing specific security services and mechanisms. ISO/IEC 10181 consists of the following parts:

  - Part 1: Security Frameworks Overview
  - Part 2: Authentication Framework
  - Part 3: Access Control Framework
  - Part 4: Confidentiality Framework
  - Part 5: Integrity Framework
  - Part 6: Non-Repudiation Framework
  - Part 7: Security Audit Framework
  - Part 8: Guide to Open Systems Security.

  – OSI Upper Layers Security Model (ISO/IEC 10745) – The Upper Layers Security Model, to be jointly assigned as ITU-T Recommendation X.803, is concerned with development of application-independent services and protocols in order to minimize the need for application-specific application service elements (ASEs) to contain internal security services. It specifies:

  - Security aspects of communication in the upper layers
  - Upper layers support of security services, as defined in the frameworks
  - Positioning and relationships of security services and mechanisms in the upper layers, in accordance with ISO 7498-2 and ISO 9545
  - Interactions among upper layers, and between upper layers and lower layers, in providing and using security services
  - Upper layer requirements for security information management.

The model does not specify:

- Security service definitions
- Security protocol specifications
- Security mechanisms, their requirements, or their protocol requirements
- Provisions for security which are not concerned with OSI communications.

The Upper Layers Security Model provides the structure for services to be defined for the session, presentation, and application layers. The Model specifically discusses the following security services:

- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Connection Integrity With Recovery
- Connection Integrity Without Recovery
- Connectionless Integrity
- Selective Field Integrity
- Entity Authentication
- Data Origin Authentication
- Access Control
- Security Labeling
- Non-Repudiation, Origin
- Non-Repudiation, Delivery
- Key Management.

– Generic Upper Layer Security (GULS) Standard (ISO/IEC 11586) – GULS specializes some of the application layer concepts of the Upper Layers Security Model to permit the exchange of security-related information between application processes in a distributed environment. GULS defines generic facilities to support construction of Upper Layer security protocols. These generic security facilities do not in themselves provide security services, but are construction tools for protocols which will provide security services for the upper layers. GULS facilities include:

- A set of notational tools to support the abstract syntax specification of selective field protection requirements, and to support the specification of *security exchanges* and *security transformations*
- A service definition, protocol specification, and PICS proforma for an application service element to support security services provided in the Application Layer
- A specification and Protocol Implementation Conformance Statement (PICS) proforma for security transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

GULS consists of six parts, including what was previously the Security Exchange Application Service Element (SE-ASE) being developed by ISO. A service element (SE) is a primitive defined at the interface between two

adjacent layers. An application service element (ASE) is a set of functions that support application programs. An ASE represents a type of work that the user expects to be performed, such as security exchanges, along with the elements needed to perform that work. The GULS parts are:

- Part 1: Overview, Models, and Notation
- Part 2: Security Exchange Service Element (SESE) Service Definition
- Part 3: SESE Protocol Specification
- Part 4: Protecting Transfer Syntax Specification
- Part 5: SESE PICS Proforma
- Part 6: Protecting Transfer Syntax PICS Proforma.

GULS facilities will support protocols which provide the following security services required by applications:

- Entity Authentication
- Data Origin Authentication
- Traffic Flow Confidentiality
- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Non-Repudiation
- Discretionary Access Control
- Mandatory Access Control
- Labeling
- Connection Integrity
- Connectionless Integrity
- Selective Field Integrity
- Key Management.

- **OSE Implementors' Workshop** – The OIW Security special interest group (SIG) were attended to acquire the current status of the NIST OSI standardization efforts. The objectives of the Security SIG are to define security architectures and implementation profiles including:

  – OSI security protocols

  – Cryptographic algorithms

  – Key management systems.

  A specific interest of the OIW is to extend the services described in the OSI Security Architecture (ISO 7498-2) to all Integrated Services Digital Network (ISDN) applications, including voice use of the public network. The security services to be provided for ISDN are access control, authentication, confidentiality, integrity, non-repudiation, service assurance, and notarization. The primary service assurance issues are capacity, redundancy, and recovery.

- **IEEE 802.10 SILS Working Group –** The Standard for Interoperable LAN and MAN Security (SILS) [IEEE 93A] is being developed by the IEEE 802.10 Working Group. Packet switched networks (PSNs) and wide area networks (WANs) were the architectural models used to develop the OSI Reference Model (ISO 7498) in 1984. The broadcast nature of LANs introduces vulnerabilities associated with subnetworks and routing that are not present in the Data Link Layer of PSNs and WANs because of their point-to-point nature. SILS will expand security services to protect LANs. SILS consists of four parts and a PICS Proforma:

  – 802.10 Clause 1 – SILS Model

  – 802.10 Clause 2 – Secure Data Exchange (SDE) Protocol

  – 802.10 Clause 3 – Key Management Protocol

  – 802.10 Clause 4 – Security Management.

  Clause 1 provides an overview for security of local area networks and metropolitan area networks, defines terms, and provides an architecture which describes the relationship of each of the security protocols to ISO 7498-2.

  Clause 2 defines the SDE Protocol to be implemented at the Data Link Layer. SDE augments standard LLC and MAC communications protocols without replacing those protocols. An SDE frame encapsulates the LLC frame and has optional fields to satisfy a broad range of security applications. SDE requires no change to the existing upper-layer protocols in the stack. SDE will operate in LANs and MANs where not all stations use SDE.

  SDE provides data confidentiality through encipherment. Connectionless integrity is provided through the use of an integrity check value (ICV). Data origin authentication is achieved through the use of the integrity service, or through the use of key management and the placement of a Station ID in the SDE protected header. Access control is provided by key management or system management.

  Clause 3 establishes a structure for key management to provide keying material and association attributes needed by security protocols at all layers. The GULS Standard services will be used to support SILS key management. Clause 3 allows asymmetric key management (via X.509 certificates), symmetric key management (ANSI X9.17), and manual keying, and addresses multicast keying.

  Clause 4 describes management functions and protocols that support the security services provided in other clauses.

  SILS provides the following security services:

  - Access Control
  - Data Origin Authentication
  - Labeling
  - Data Confidentiality
  - Connectionless Integrity
  - Key Management.

- **Internet Engineering Task Force (IETF)** – The IETF began as a forum for technical coordination by contractors for the Defense Advanced Research Projects Agency (DARPA), working on the ARPANET, Defense Data Network (DDN), and the Internet core gateway system. The first IETF meeting was held in 1986 with 15 attendees. Since that time, the Internet has grown to more than six million host computers and 60 million users, and is currently doubling in size every six months. Attendance at the IETF is proportional, with just under 1,000 attendees at the last meeting. There are four groups in the IETF structure:

  – Internet Society (ISOC) and Board of Trustees – responsible for Internet growth, evolution, standardization, and usage (social, political, and technical)

  – Internet Architecture Board (IAB) – the ISOC technical advisory group; oversees two Task Forces: IETF, which considers near-term problems, and Internet Research Task Force (IRTF), which considers long-term problems

  – Internet Engineering Steering Group (IESG) – consists of the directors of each of the IETF functional areas and the IETF Chair. Responsible for technical management of IETF activities and the Internet Standards process

  – IETF itself – proposes solutions to technical Internet problems, specifies protocols and near-term architectures, recommends their standardization to the IESG, and provides a forum for information exchange. The IETF is divided into ten Functional Areas, one of which is the Security Area. The number of Working Groups within the Security Area increases at almost every IETF meeting. Currently, there are 10 Security Area Work Groups, with the likelihood that one more will be added in July. They are:

    - Security Area Advisory Group (saag)
    - Internet Protocol Security Protocol (ipsec)
    - Common Authentication Technology (cat)
    - Domain Name System Security (dnssec)
    - Privacy Enhanced Mail (pem)
    - Authorization and Access Control (aac)
    - Commercial IP Security Option (cipso)
    - Independent Object/Document Security (ios)
    - Authenticated Firewall Traversal (aft)
    - Web Transport Security
    - S/Key One-Time Password.

Section 3

Proposed Direction for Future Work Efforts

This Page Intentionally Left Blank

3.0 Proposed Direction for Future Work Efforts

Networking technology has evolved significantly over the past few years and the mission of the SPAWAR INFOSEC Office (PD71) has evolved to keep pace with it. PD71 is charged with the responsibility of being the single point of contact for Navy, Marine Corps, and Coast Guard for the planning, development, acquisition, fielding, and life-cycle support of standard INFOSEC products. Network operating systems provide a wide range of client-server security features, yet they do not meet all of the Navy's security needs nor those of commercial organizations processing highly sensitive data.

An area that stands out as a problem for some commercial and Navy organizations is the protection of Sensitive Unclassified information on LANs. Another problem commercial and Government organizations face is that they are assigning inexperienced personnel to set up, provide security for, and manage their networks. In addition, many personnel who are adequately trained rotate on to new assignments, leaving inadequately trained replacements to administer the networks.

Phase II began the effort of providing security management guidance to NetWare administrators. This supports the SPAWAR Chief Engineer's missions of recommending security designs and implementation alternatives and providing security documentation reviews and support. It also supports the SPAWAR Customer Service Division missions to provide system security support, translate INFOSEC threats into security enhancements, and develop INFOSEC training programs.

It has been proposed that the SBIR Phase III effort focus on the Sensitive Unclassified environment in support of these PD71 missions.

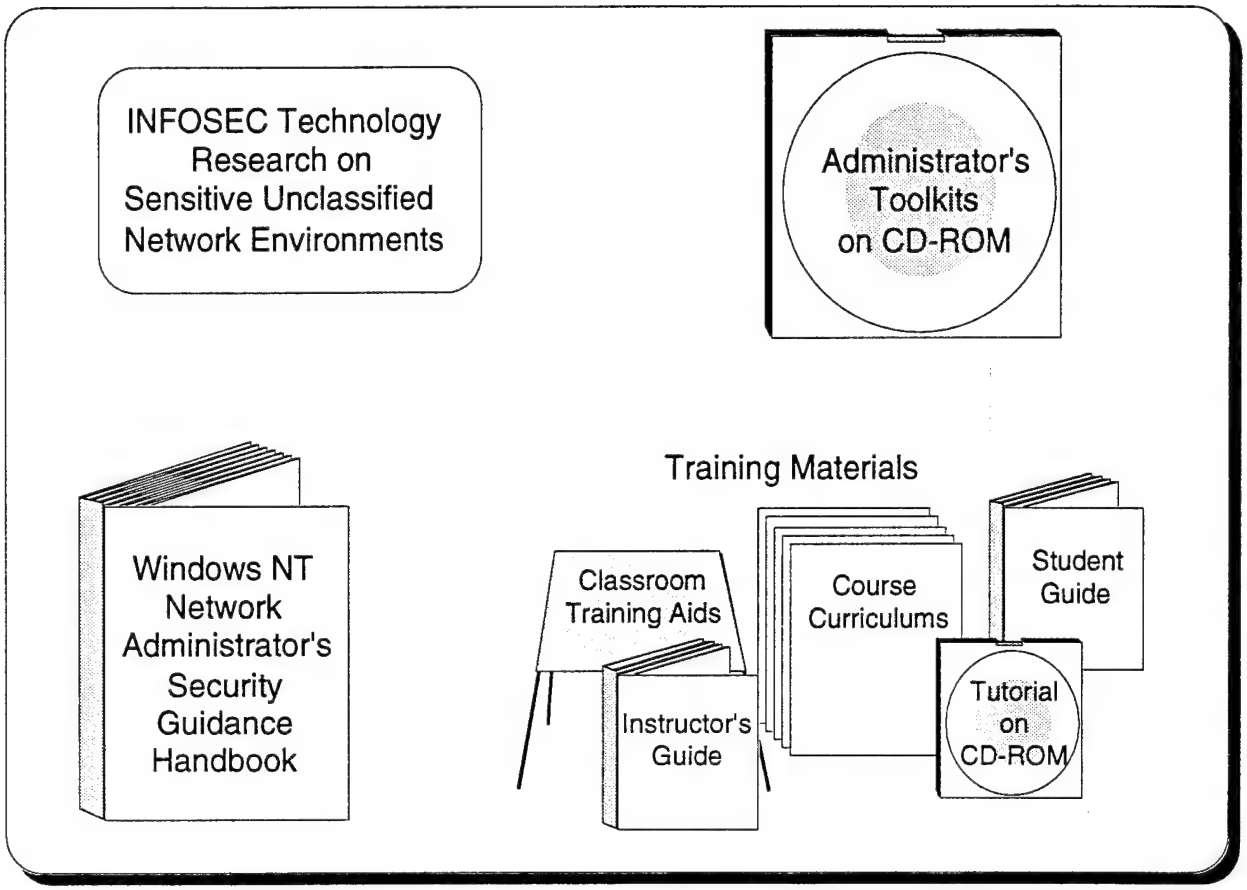

Figure 3-1. SBIR Phase III Objectives

The Phase III proposal calls for Secure Solutions to develop a comprehensive set of network security administration tools for recently assigned Novell NetWare administrators in commercial and Government organizations. It has also been proposed that Phase III tasking be broadened to include support of Windows NT environments since the recently introduced Windows NT is rapidly becoming widely implemented as well.

The products would provide guidance materials and security administration tools to help the inexperienced administrators who understand the mechanics of activating NetWare and Windows NT user accounts and establishing rights and privileges, but who lack security training for sensitive environments and need support tools and guidance concerning which security features to implement and which third-party products to install on the network. The tools would also support administrators with more security experience but who lack some specific knowledge such as knowledge of firewalls. In addition, the Phase III products can be used to brief management on security, resource, and funding needs.

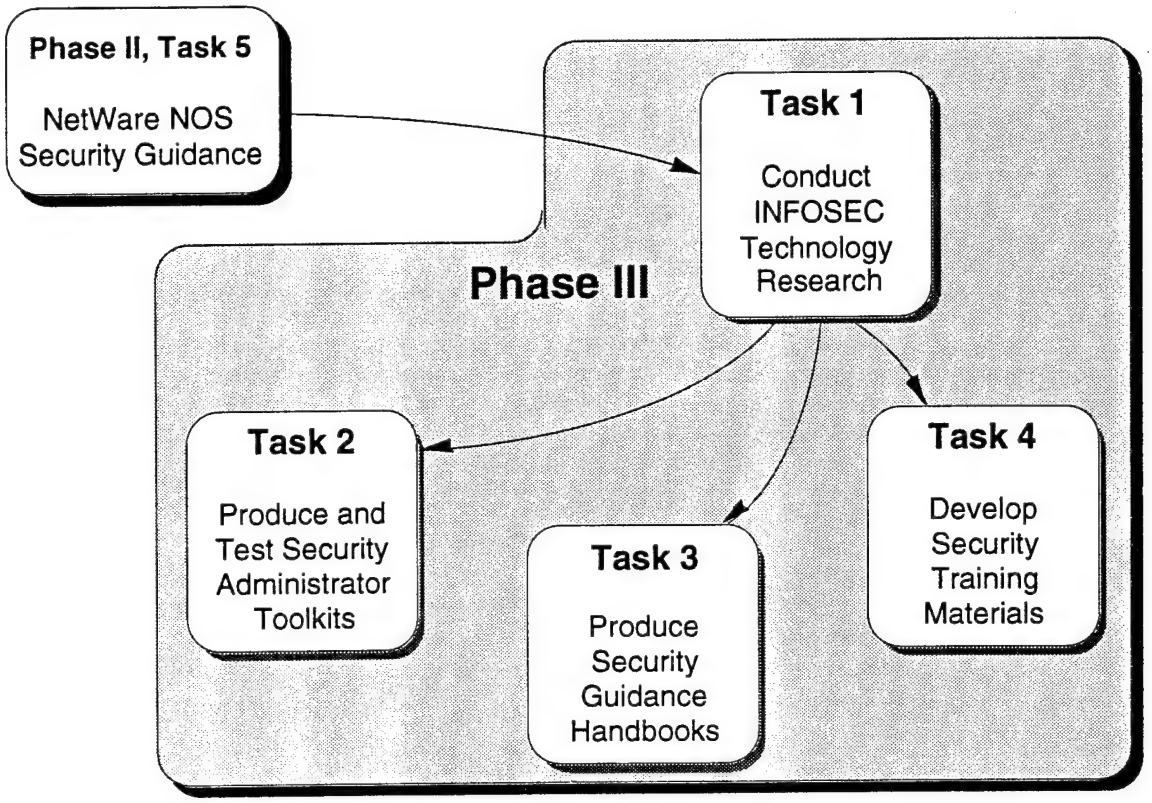

Figure 3-2. SBIR Phase III Task Relationships

The following tasks are proposed for Phase III:

- **Conduct INFOSEC research** – Conduct INFOSEC technology research to determine requirements for Sensitive Unclassified information network environments

- **Produce *Security Administrator Toolkits*** – Serve as a system integrator/broker for the Navy in the design, development, and testing of security administrator toolkits consisting of security and test tools, information resources, and a HyperText graphical user interface on CD-ROM

- **Produce *Windows NT Security Guidance Handbook*** – Develop a Windows NT Administrator's Security Guidance Handbook which recommends options for securing Windows NT LANs in commercial and Government Sensitive Unclassified environments. The handbook will be modeled after the NetWare Administrator's Security Guidance Handbook developed during Phase II

- **Develop *Security Training Materials*** – Develop training materials (e.g., user and administrator training requirements, course curriculum, instructor's guide, classroom training aids, student's guide, tutorials on CD-ROM, testing materials, and course evaluation forms) for commercial and Navy organizations to convey security information to NetWare and Windows NT users and administrators.

This Page Intentionally Left Blank

Appendices

This Page Intentionally Left Blank

Appendix A

Acronyms

This Page Intentionally Left Blank

Appendix A

Acronyms

ALLPOWER	All Purpose Workstation Security Peripheral
ANSI	American National Standards Institute
API	Application Programming Interface
ARPANET	Advanced Research Project Agency Network
ASE	Application Service Element
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
C4I	Command & Control, Communications & Computers, and Intelligence
CD-ROM	Compact Disk - Read Only Memory
CLNP	Connectionless Network Protocol
CMIP	Common Management Information Protocol
COTS	Commercial Off-The-Shelf
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DARPA	Defense Advanced Research Projects Agency
DCE	Data Circuit-terminating Equipment
DGSA	DoD Goal Security Architecture
DISSP	DoD Information Systems Security Policy
DoD	Department of Defense
DQDB	Distributed Queue Dual Bus
DTE	Data Terminal Equipment
E3	End-to-End Encryption
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FTAM	File, Transfer, Access and Management Protocol
FTP	File Transfer Protocol
GLOBIXS	Global Information Exchange System
GOSIP	Government OSI Profile
GOTS	Government Off-The-Shelf
GULS	Generic Upper Layer Security
IAB	Internet Architecture Board
IC2	Integrated Interior Communications System
ICV	Integrity Check Value
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
INFOSEC	Information Security
IP	Internet Protocol
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISO	International Standards Organization

Appendix A – Acronyms (continued)

ISOC	Internet Society
KMP	Key Management Protocol
LAN	Local Area Network
LAPB	Link Access Procedures – B
LLC	Logical Link Control
LOCK™	Logical Coprocessing Kernel
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MISSI	Multilevel Information Systems Security Initiative
MLS	Multilevel Security
MSP	Message Security Protocol
NCCOSC	Naval Command, Control, and Ocean Surveillance Center
NDS	NetWare Directory Services
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NOS	Network Operating System
NRaD	NCCOSC RDTE Division
NRL	Naval Research Laboratory
NSA	National Security Agency
NSWC	Naval Surface Warfare Center
OIW	OSE Implementors' Workshop
OSE	Open Systems Environment
OSI	Open Systems Interconnection
OSI RM	OSI Reference Model
PCI	Protocol Control Information
PCMCIA	Personal Computer Memory Card International Association
PDU	Protocol Data Unit
PDS	Protected Distribution System
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PICS	Protocol Implementation Conformance Statement
PSN	Packet Switched Network
SBIR	Small Business Innovation Research
SDE	Secure Data Exchange Protocol
SDNS	Secure Data Network System
SE	Service Element
SESE	Security Exchange Service Element
SILS	Standard for Interoperable LAN and MAN Security
SMDS	Switched Multimegabit Data Service
SMIB	Security Management Information Base
SMP	Security Management Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

Appendix A – Acronyms (continued)

SONET	Synchronous Optical Network
SP2L	Security Protocol 2 for LANs
SP3	Security Protocol 3
SP4	Security Protocol 4
SP7	Security Protocol 7
SPAWAR	Space and Naval Warfare Systems Command
TADIXS	Tactical Data Information Exchange System
TCP	Transmission Control Protocol
TLSP	Transport Layer Security Protocol
TP0	Connection Oriented Transport Protocol, Class 0
TP1	Connection Oriented Transport Protocol, Class 1
TP2	Connection Oriented Transport Protocol, Class 2
TP3	Connection Oriented Transport Protocol, Class 3
TP4	Connection Oriented Transport Protocol, Class 4
UDP	User Datagram Protocol
VLM	NetWare Virtual Loadable Module
WAN	Wide Area Network

This Page Intentionally Left Blank

Appendix B

References

This Page Intentionally Left Blank

Appendix B

References

[ADAMS 94] Adams, C., "Security Initiative for Defense Nets Takes Small Steps Forward," *Federal Computer Week,* July 25, 1994, pp. 20-22.

[ANSI 88A] American National Standards Institute, *Digital Hierarchy – Optical Interface Rates and Formats Specification,* ANSI T1.105-1988, (Synchronous Optical Network – SONET), ANSI T1X1.5, 1988.

[ANSI 88B] American National Standards Institute, *Digital Hierarchy – Optical Parameters,* ANSI T1.106-1988, (SONET), ANSI T1X1.5, 1988.

[ANSI 89] American National Standards Institute, *Addendum to ANSI T1-105-1988, Digital Hierarchy – Optical Interface Rates and Formats Specification, (Phase 2 SONET),* ANSI T1X1.5, 1989.

[ANSI 92A] American National Standards Institute, *Information Resource Dictionary System (IRDS) Services Interface,* ANSI Standard X3.185-1992 (ISO 10728), 1992.

[ANSI 92B] American National Standards Institute, *Frame Relay Bearer Service Architectural Framework and Service Description,* draft standard T1.606, 1992, (aligned with CCITT Q.922).

[ANTHES 94] Anthes, Gary, "Poll finds security less than passable," *Computerworld,* Volume 28, Issue 16, April 18, 1994, pp. 63.

[BAILEY 93] Bailey, B., "Trends in Networking," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-259 – S-266.

[BAKER 95] Baker, Richard H., *Network Security – How to Plan For It and Achieve It,* McGraw-Hill, New York, NY, 1995.

[BALLOU 93] Ballou, Melinda C., "UnixWare, NetWare Blend Questioned," *Computerworld,* Volume 27, Number 29, July 19, 1993, pp. 14.

[BARKER 89] Barker, L. K., "Network Management and Diagnostics for Secure LANs," *Local Area Network Security, Lecture Notes in Computer Science 396, Springer-Verlag,* 1989, pp. 139-152.

Appendix B – References (continued)

[BLACK 91] Black, Uyless, *OSI – A Model for Computer Communications Standards,* Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[BLACK 92A] Black, Uyless, *Network Management Standards – The OSI, SNMP and CMOL Protocols,* McGraw-Hill, New York, New York, 1992.

[BLACK 92B] Black, Uyless, *TCP/IP and Related Protocols,* McGraw-Hill, New York, New York, 1992.

[BLACK 93A] Black, Uyless, *Computer Networks – Protocols, Standards, and Interfaces,* Second Edition, Prentice Hall, Englewood Cliffs, New Jersey, 1993.

[BLACK 93B] Black, Uyless, *Data Link Protocols,* Prentice Hall, Englewood Cliffs, New Jersey, 1993.

[BOCKEN 94] Bockenski, Barbara, *Implementing Production-Quality Client/Server Systems,* John Wiley & Sons, New York, NY, 1994.

[BUSSE 93] Busse, Torsten, "Intel Beefs Up Features of LANDesk Manager – NLMs Offer Node Data, Security," *Infoworld,* Volume 15, Number 25, June 21, 1993, pp. 45.

[CCITT 88] The International Telegraph and Telephone Consultative Committee (CCITT), *Recommendation X.25, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuits,* 1988.

[CCITT 91] The International Telegraph and Telephone Consultative Committee (CCITT), *Broadband Integrated Services Digital Network (B-ISDN) Asynchronous Transfer Mode (ATM) Functional Characteristics,* Recommendation I.150, 1991.

[CCITT 92] The International Telegraph and Telephone Consultative Committee (CCITT), *ISDN Data Link Layer Specification for Frame Mode Bearer Services,* Recommendation Q.922, 1992.

[CHAP 92] Chapman, D. Brent, "Network (In) Security Through IP Packet Filtering," *USENIX Security Symposium III Proceedings,* USENIX Association, Baltimore, MD, September 14-16, 1992.

[CHAP 95] Chapman, D. Brent, and Elizabeth D. Zwicky, *Building Internet Firewalls,* O'Reilly and Associates, New York, NY, 1995. *(Note: this book is due for release on September 18, 1995)*

Appendix B – References (continued)

[CHES 94] Cheswick, William R. and S.M. Bellovin, *Firewalls and Internet Security - Repelling the Wily Hacker,* Addison-Wesley, Reading, MA, 1994.

[CHIU 92] Chiu, Dah Ming and Ram Sudama, *Network Monitoring Explained – Design and Applications,* Ellis Horwood Limited, Cirencester, England, 1992.

[CHORA 94] Chorafas, Dimitris N., *Beyond LANS – Client/Server Computing,* McGraw-Hill, New York, NY, 1994.

[CLARK 87] Clark, D.D., and D.R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proceedings of the 1987 IEEE Symposium on Security and Privacy,* April 1987.

[CLIPPER 93] Mykotronx, Inc., *Clipper Family: A New Breakthrough in Encryption Technology,* October 1993.

[CNO 93] Chief of Naval Operations, *Sonata Overview,* circa June 1993.

[COMER 91] Comer, D.E., *Internetworking With TCP/IP, Volume I: Principles, Protocols, and Architecture,* Second Edition, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[COOPER 95] Cooper, F.J., et al., *Implementing Internet Security,* New Riders Publishing, Indianapolis, Indiana, 1995.

[COOPERS 94A] Coopers & Lybrand, *Novell NetWare – Security, Audit, and Control,* presentation notes, Information Systems Audit and Control Association Mid-Atlantic Audit & Control Conference, September 14, 1994.

[COOPERS 94B] Coopers & Lybrand, *Microsoft Windows NT 3.5 – Guidelines for Security, Audit, and Control,* Microsoft Press, Redmond, Washington, 1994.

[COURSEY 93] Coursey, David, "In Need of Novell," *Computerworld,* Volume 27, Number 35, August 30, 1993, pp. 60.

[CRAW 93] Crawford, Tim M., "Install a Secret Back Door to Your Server," *Infoworld,* Volume 15, Number 40, October 4, 1993, pp. 125.

[DALY 92] Daly, James, "Antivirus Utility for NetWare Servers Due," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 4.

Appendix B – References (continued)

[DALY 93A] Daly, James, "Applications Offer Central Net Security," *Computerworld,* Volume 27, Number 31A, August 9, 1993, pp. 62.

[DALY 93B] Daly, James, "Open Security: Resolving the Paradox," *Computerworld,* Volume 27, No. 31A, August 11, 1993, pp. 22-26.

[DALY 93C] Daly, James, "Put a Sentry On Your LAN," *Computerworld,* Volume 27, Number 41, October 11, 1993, pp. 44.

[DAVIS 94A] Davis, Peter T., *Complete LAN Security and Control,* McGraw-Hill, New York, NY, 1994.

[DAVIS 94B] Davis, Peter T., *Manager's Guide to Internet Security,* Computer Security Institute, San Francisco, CA, 1994.

[DAY 92] Day, Michael, *Enterprise Series: Downsizing to NetWare,* New Riders Publishers, Carmel, Indiana, 1992.

[DCA 91] Defense Communications Agency, MLS Technology Insertion Program, *Technical Memorandum – Target Architecture and Implementation Strategy for the Joint MLS Technology Insertion Program,* March 1991.

[DECISIS 94] Decisis, Inc., *1995 Guide to Switched Internetworking Technologies,* Decisis, Inc., Herndon, VA, 1994.

[DEWIRE 94] Dewire, Dawna T., *Application Development for Distributed Environments,* McGraw-Hill, New York, NY, 1994.

[DGSA 93] Center for Information System Security, Defense Information System Security Program (DISSP), *Department of Defense (DoD) Goal Security Architecture (GOAL), Version 1.0,* Draft, Aug 1, 1993.

[DIGIRO 91] DiGirolamo, V., *Naval Command and Control: Policy, Programs, People & Issues,* AFCEA International Press, 1991 (forward by Vice Admiral Jerry O. Tuttle).

[DISA 93] Defense Information Systems Agency, Joint Interoperability and Engineering Organization, *Standard Mail Guard (SMG) Functional Requirements Document,* Coordination Draft, October 29, 1993.

[DoD 85] Department of Defense, *Trusted Computer System Evaluation Criteria (TCSEC),* DoD 5200.28-STD, December 1985.

Appendix B – References (continued)

[DoD 91] Department of Defense, *Military Standard – Network Management for DoD Communications,* MIL-STD-1813, unapproved working draft, June 10, 1991, (superseded by MIL-STD-2045-38000 [DoD 93A]).

[DoD 93A] Department of Defense, *Military Standard – Network Management for DoD Communications,* MIL-STD-2045-38000, (supersedes MIL-STD-1813 [DoD 91]), unapproved working draft, January 4, 1993.

[DoD 93B] Department of Defense, *Military Handbook – Network Management for DoD Communications,* MIL-HDBK-1351, unapproved working draft, undated, approximate publication date: November 1993.

[DOSTER 92A] Dostert, Michele, "Microsoft, Novell Square Off," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 6.

[DOSTER 92B] Dostert, Michele, "Novell Issues Network Security Patch – Device Will Guard Against LAN Break-ins But Not Careless Users," *Computerworld,* Volume 26, Number 47, November 23, 1992, pp. 4.

[ELLISON 92] Ellison, Craig, "Intel Joins the Network Virus Hunt with LANProtect," *PC Magazine,* Volume 11, Number 1, June 16, 1992, pp. 50.

[FATAH 94] Fatah, Burhan, *Electronic Mail Systems – A Network Manager's Guide,* McGraw-Hill, New York, NY, 1994.

[FIREFOX 95] Firefox, Inc., *Internet Security: Solutions for the NetWare Environment,* Firefox, Inc., San Jose, CA, March 1995.

[FORD 94] Ford, Warwick, *Computer Communications Security – Principles, Standard Protocols and Techniques,* Prentice Hall, Englewood Cliffs, NJ, 1994.

[FRAME 90] Frame Relay Consortium: DEC, Northern Telecom Inc., and StrataCom Inc., *Frame Relay Specification with Extensions Based on Proposed T1S1 Standards, Revision 1,* Document Number 001-208966, September 18, 1990.

[FRYER 94] Fryer, Bronwyn, "Virus Protection: At Your Server," *Computerworld,* Volume 28, Number 18, May 2, 1994, pp. 121.

[GASSER 88] Gasser, Morrie, *Building a Secure Computer System,* Van Nostrand Reinhold Company, New York, 1988.

[GASSER 91] Gasser, Morrie, *Security in Distributed Systems,* 1991.

Appendix B – References (continued)

[GHIGG 93] Ghiggino, Pierpaolo and Charles A. Eldering, Editors, *Local and Metropolitan Area Networks,* SPIE – The International Society for Optical Engineering, Bellingham, WA, 1993.

[GOSIP 93] The GOSIP Institute, *Internet 2000: A Protocol Framework to Achieve a Single Worldwide TCP/IP/OSI/CLNP Internet by Year 2000, A White Paper, Version 3.0,* June 4, 1993.

[GRUM 92] Grumman Data Systems, *Secure SAFENET Communications,* NRaD Contract N66001-90-D-0192, June 30, 1992.

[HALSALL 92] Halsall, Fred, *Data Communications, Computer Networks and Open Systems, Third Edition,* Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[HAMPTON 93] Hampton, William R., "Improving LAN Security and Auditing Using Novell NetWare Version 4.0," *Computer Security Journal,* Volume 9, Number 2, Fall 1993, pp. 37-47.

[HARBAUG 93] Harbaugh, Logan G., *Novell's Problem-Solving Guide to NetWare Systems,* Novell Press, San Jose, CA, 1993.

[HEALY 89] Healy, E.M., "SONET Overview and Standards Status," *Proceedings of the IEEE SONET Symposium,* November 1989.

[HEBRAWI 93] Hebrawi, B., *Open Systems Interconnection – Upper Layer Standards and Practices,* McGraw-Hill, New York, New York, 1993.

[HELD 94] Held, Gilbert, *Token-Ring Networks: Characteristics, Operations, Construction, and Management,* John Wiley & Sons, New York, NY, 1994.

[HERBON 94] Herbon, Gamal, *Designing NetWare Directory Services,* Henry Holt and Company, New York, NY, 1994.

[HOFFMAN 93] Hoffman, Thomas, "Novell Leads Client/Server Security Effort," *Computerworld,* Volume 27, Number 29, July 19, 1993, pp. 14.

[HORWITT 93] Horwitt, Elizabeth, "Interop '93 Unveilings – Products Demonstrate Vendors' Commitment to SNMP Systems, Interoperability Across Systems," *Computerworld,* Volume 27, Number 35, August 30, 1993, pp. 59.

[HORWITT 94] Horwitt, Elizabeth, "LAN/Mainframe Security Addressed," *Computerworld,* Volume 28, Number 12, March 21, 1994, pp. 69.

Appendix B – References (continued)

[HUNTER 93] Hunter, Philip, *Local Area Networks – Making the Right Choices,* Addison-Wesley, Reading, Massachusetts, 1993.

[IEEE 88] Institute of Electrical and Electronics Engineers, *IEEE Standard Portable Operating System Interface for Computer Environments (POSIX),* IEEE Std 1003.1-1988, August 22, 1988.

[IEEE 90] Institute of Electrical and Electronics Engineers, *IEEE Standard for Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network,* IEEE Standard 802.6, 1990.

[IEEE 92A] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Logical Protocol Specification,* IEEE Standard 896.1-1991, March 10, 1992. (Amended in 1993. Became ISO 10857 in 1994.)

[IEEE 92B] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Physical Layer and Profile Specification,* IEEE Standard 896.2-1991, April 24, 1992.

[IEEE 92C] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Recommended Practices,* Unapproved Draft IEEE Standard P896.3/D4.1, IEEE Computer Society, October 1992.

[IEEE 92D] Institute of Electrical and Electronics Engineers, *Draft Standard for Information Technology -- Portable Operating System Interface (POSIX) -- Part 1: System Application Program Interface (API) Amendment #: Protection, Audit and Control Interfaces,* Unapproved Draft IEEE P1003.6.1/D13, November 1992.

[IEEE 92E] Institute of Electrical and Electronics Engineers, *Draft Standard for Information Technology -- Portable Operating System Interface (POSIX) -- Part 2: Shell and Utilities – Amendment #: Protection and Control Utilities,* Unapproved Draft IEEE P1003.6.2/D13, November 1992.

[IEEE 93A] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS),* Currently Contains Secure Data Exchange (SDE) (Clause 2), IEEE Standard 802.10-1992, February 5, 1993.

[IEEE 93B] Institute of Electrical and Electronics Engineers, *IEEE Standard for Scalable Coherent Interface (SCI),* IEEE Standard 1596-1992, August 2, 1993.

Appendix B – References (continued)

[IEEE 93C] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Profile M (Military),* IEEE Standard 896.5-1993, 1993.

[IEEE 94] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) Clause 3 — Key Management Protocol,* Unapproved Draft IEEE 802.10c/D5, June 8, 1994.

[IEEE 95] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) - Secure Data Exchange Security Labels (SDE-SL),* Unapproved Draft IEEE 802.10g/D7, March 1, 1995.

[INFOSEC 94] "Encryption: Scramble Data to Protect It," *Infosecurity News,* November/December, 1994, pp. 82-91.

[ISO 84] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model,* ISO 7498, October 1984.

[ISO 88A] International Standards Organization, *Information Processing Systems—Open Systems Interconnection — File Transfer, Access, and Management – Part 1: General Introduction,* ISO 8571, October 1988.

[ISO 88B] International Standards Organization, *Information Processing Systems—Open Systems Interconnection — Connection Oriented Transport Protocol Specification,* ISO 8073, December 15, 1988.

[ISO 89A] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture,* ISO 7498-2, February 1989; also ITU-T Recommendation X.800.

[ISO 89B] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 1: Physical Layer Protocol (PHY),* ISO 9314-1, April 1989.

[ISO 89C] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 2: Token Ring Media Access Control,* ISO 9314-2, June 1989.

Appendix B – References (continued)

[ISO 90A] International Standards Organization, *Information Processing Systems—Fiber Distributed Data Interface (FDDI)— Part 3: Physical Layer Medium Dependent (PMD),* ISO 9314-3, October 1990.

[ISO 90B] International Standards Organization, *Information Processing Systems—Local Area Networks— Part 4: Token-Passing Bus Access Method and Physical Layer Specification,* ISO/IEC 8802-4, 1990; ANSI/IEEE Std 802.4.

[ISO 90C] International Standards Organization, *Information Processing Systems—Data Communications – X.25 Packet Level Protocol for Data Terminal Equipment,* ISO 8208, 1990; also CCITT Recommendation X.25.

[ISO 90D] International Standards Organization, *Information Processing Systems—Common Management Information Protocol Specification,* ISO 9596, 1990.

[ISO 90E] International Standards Organization, *Information Processing Systems — Local Area Networks — Part 2: Logical Link Control,* ANSI/IEEE Std 802.2, ISO 8802-2, January 12, 1990 (also ITU-T Recommendation X.810).

[ISO 90F] International Standards Organization, *Information Technology — Text Communication, Message-Oriented Text Interchange System — Part 1: System and Service Overview,* ISO 10021-1, Dec. 1990.

[ISO 90G] International Standards Organization, *Information Processing Systems — The Directory — Part 8: Directory Authentication,* ISO 9594-8, 1990.

[ISO 90H] International Standards Organization, *Information Technology – Portable Operating System Interface (POSIX) – Part 1: System Application Program Interface (API) [C Language],* ISO/IEC 9945-1, December 7, 1990. (Cross Reference: IEEE Std 1003.1)

[ISO 92A] International Standards Organization, *Information Technology — Local and Metropolitan Area Networks – Part 5: Token Ring Access Method and Physical Layer Specification,* ISO/IEC 8802-5, 1992; ANSI/IEEE Std 802.5.

[ISO 92B] International Standards Organization, *Information Technology — Protocol for Providing the Connectionless-Mode Network Service,* ISO/IEC 8473-1, 1992; also ITU-T Recommendation X.233.

Appendix B – References (continued)

[ISO 92C] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Guide to Open Systems Security,* Working Draft Technical Report, May 1992.

[ISO 92D] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 5: Hybrid Ring Control,* ISO 9314-5, (FDDI-II), JTC1 Project Draft, 1992.

[ISO 92E] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol,* ISO/IEC 10736, December 18, 1992

[ISO 92F] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Network Layer Security Protocol,* ISO 11577, November 29, 1992.

[ISO 92G] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol (Amendment 1 - Security Association Protocol),* Revised Draft, December 22, 1992.

[ISO 93A] International Standards Organization, *Information Processing Systems – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification,* ISO/IEC 8802-3, 1993; ANSI/IEEE Std 802.3.

[ISO 93B] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 1: Overview, Models and Notation,* ISO/IEC 11586-1, 1993.

[ISO 93C] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 2: Security Exchange Service Element (SESE) Service Definition,* ISO/IEC 11586-2, 1993.

[ISO 93D] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 3: Security Exchange Service Element Protocol Specification,* ISO/IEC 11586-3, 1993.

Appendix B – References (continued)

[ISO 93E] International Standards Organization, *Information Technology – Information Retrieval, Transfer and Management for OSI, Generic Upper Layer Security (GULS) – Part 4: Protecting Transfer Syntax Specification,* ISO/IEC 11586-4, 1993.

[ISO 93F] International Standards Organization, *Information Processing Systems — Remote Database Access (RDA),* ISO/IEC DIS 9579, 1993.

[ISO 93G] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Lower Layers Security Model,* Working Draft, Proposed Technical Report, August 1993.

[ISO 93H] International Standards Organization, *Information Processing Systems — Reference Model of Data Management,* ISO 10032, December 1993.

[ISO 93J] International Standards Organization, *Information Technology — Portable Operating System Interface (POSIX) – Part 2: Shell and Utilities,* ISO/IEC 9945-2, 1993.

[ISO 94A] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 1: Security Frameworks Overview,* ISO/IEC 10181-1, 1994.

[ISO 94B] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 2: Authentication Framework,* ISO/IEC 10181-2, January 1994 (also ITU-T Recommendation X.811).

[ISO 94C] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 3: Access Control Framework,* ISO/IEC 10181-3, January 1994 (also ITU-T Recommendation X.812).

[ISO 94D] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 4: Confidentiality Framework,* ISO/IEC 10181-4, 1994 (also ITU-T Recommendation X.813).

Appendix B – References (continued)

[ISO 94E] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 5: Integrity Framework,* ISO/IEC 10181-5, 1994 (also ITU-T Recommendation X.814).

[ISO 94F] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems–Part 6: Non-repudiation Framework,* ISO/IEC 10181-6, 1994 (also ITU-T Recommendation X.815).

[ISO 94G] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 7: Security Audit Framework,* ISO/IEC 10181-7, 1994 (also ITU-T Recommendation X.816).

[ISO 94H] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 8: Guide to Open Systems Security,* ISO/IEC 10181-8, 1994.

[ISO 94J] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Network Layer Security Protocol,* ISO/IEC 11577, Final text accepted November 1993. International standard published 1994.

[ISO 94K] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol,* ISO/IEC 10736, Final text accepted November 1993. International standard published 1994.

[ISO 94L] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol (Amendment 1 - Security Association Protocol),* Final text accepted November 1993. International standard published 1994.

[ISO 94M] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Upper Layers Security Model,* ISO/IEC 10745, 1994 (also ITU-T Recommendation X.803).

[ISO 94N] International Standards Organization, *Information Technology — Futurebus+ – Logical Protocol Specification,* ISO/IEC 10857, 1994 (also IEEE 896.1-1993).

Appendix B – References (continued)

[ITU 91] International Telecommunications Union – Telecommunications Sector (formerly CCITT), *Broadband Integrated Services Digital Network (B-ISDN) Asynchronous Transfer Mode (ATM) Functional Characteristics,* Recommendation I.150, 1991.

[ITU 92] International Telecommunications Union – Telecommunications Sector (formerly CCITT), *Integrated Services Digital Network (ISDN) Data Link Layer Specification for Frame Mode Bearer Services,* Recommendation Q.922, 1992.

[JOHNSON 94] Johnson, Johna T., "The Internet: Corporations Worldwide Make the Connection," *Data Communications,* Volume 23, Number 6, April, 1994, pp. 66-78.

[JOST 92] Jost, Marty, *NetWare – The Macintosh Connection,* Windcrest-McGraw-Hill, Blue Ridge Summit, PA, 1992.

[JSC 94] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence,* February 28, 1994.

[KAPLAN 95] Kaplan, Jon, "Unscrambling the Secret of Encryption," *Security Management,* Volume 39, Number 2, February, 1995, pp. 67-70.

[KARAN 95] Karanjit, Siyan, *Internet Firewalls and Network Security,* New Riders Publishing, Indianapolis, Indiana, 1995.

[KAVAN 95] Kavanagh, Paul, *Downsizing for Client/Server Applications,* Academic Press Professional, Cambridge, MA, 1995.

[KING 94] King, Adrian, "Examining the Peer-to-Peer Connectivity and Multiple Network Support of Chicago," *Microsoft Systems Journal,* Volume 9, Number 11, November, 1994, pp. 15-30.

[KIRKPAT 89] Kirkpatrick, K.E., "Why is a LAN a LAN?," *Local Area Network Security, Lecture Notes in Computer Science 396, Springer-Verlag,* 1989, pp.3-4

[KIRKPAT 91] Kirkpatrick, K.E., "OSI-Based LAN Security Standards," *Handbook of Local Area Networks,* Auerbach Publications, Boston Massachusetts, 1991, pp. 741-753

[LAMBERT 89] Lambert, Paul A., "Architectural Considerations for LAN Security Protocols," *Local Area Network Security, Lecture Notes in Computer Science 396, Springer-Verlag,* 1989, pp. 5-11.

Appendix B – References (continued)

[LAMBERT 90] Lambert, Paul A., "The Lowdown on Lower Layer Security Protocols," *Proceedings of the Sixth Annual Computer Security Applications Conference,* December 1990.

[LAMBERT 93] Lambert, Paul A., "Layer Wars: Protect the Internet with Network Layer Security," *Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* February 1993.

[LAUBACH 93] Laubach, Edwin G., et al., *Networking with Banyan VINES, Second Edition,* McGraw-Hill, New York, NY, 1993.

[LAWREN 93] Lawrence, Bill, et al., *Using Novell NetWare 4 – Special Edition,* Que Corporation, New York, NY, 1993.

[LAWREN 94] Lawrence, Bill, et al., *Using NetWare 3.12 – Special Edition,* Que Corporation, New York, NY, 1994.

[LIEBING 93] Liebing, Edward, *NetWare User's Guide, Versions 3.11 and 3.12,* Henry Holt and Company, New York, NY, 1993.

[LYNCH 93] Lynch, D.C., and M. T. Rose, editors, *Internet System Handbook,* Addison-Wesley Publishing Company, Greenwich, Connecticut, 1993.

[MADRON 92] Madron, Thomas W., *Network Security in the '90s – Issues and Solutions for Managers,* John Wiley & Sons, New York, NY, 1992.

[MALAMUD 92] Malamud, Carl, *Stacks – Interoperability in Today's Computer Networks,* Prentice Hall, Englewood Cliffs, New Jersey, 1992.

[MARSH 94] Marshall, Brian, *Using Windows NT: The Essentials for Professionals,* Prentice-Hall, Englewood Cliffs, NJ, 1994.

[MARTIN 94] Martin, James, *Local Area Networks – Architectures and Implementations, Second Edition,* Prentice Hall, Englewood Cliffs, NJ, 1994.

[MAUGHAN 92] Maughan, W.D., *Standards for Computer Systems Security: An Interoperability Analysis of SDNS SP3 and ISO NLSP,* April 15, 1992.

[MCCAR 93] McCarthy, Vance, "NetWare Add-in Closes Password Detection Loophole On Small LANs," *Infoworld,* Volume 15, Number 36, September 6, 1993, pp. 8.

Appendix B – References (continued)

[MEREN 94] Merenbloom, Paul, "LAN Talk – Some Tips For Smoothly Upgrading Your Server to NetWare 4," *Infoworld,* Volume 16, Number 21, May 23, 1994, pp. 94.

[MIAST 93] Miastkowski, Stan and Anne Fischer Lent, *The Windows for Workgroups Bible,* Addison-Wesley, Reading, MA, 1993.

[MICHAEL 93] Michael, W.H., W.J. Cronin, and K.F. Pieper, *FDDI: An Introduction to Fiber Distributed Data Interface,* Digital Press, Burlington, Massachusetts, 1993.

[MICRO 92] Microsoft Corporation, *WG0667: Peer-to-Peer vs. Client-Server Networks, Application Notes – Windows for Workgroups Version 3.1 Resource Kit,* 1992.

[MINASI 95] Minasi, Mark, et al., *Mastering Windows NT Server 3.5,* Sybex, Alameda, CA, 1995.

[MISSI 93A] MISSI Program Office (NSA), *MISSI System Architecture,* FOUO, March 17, 1993.

[MISSI 93B] MISSI Program Office (NSA), *System Security Framework for the Multilevel Information System Security Initiative (MISSI),* FOUO, Draft, April 20, 1993.

[MISSI 93C] MISSI Program Office (NSA), *Multilevel Information Systems Security Program,* FOUO, August 3, 1993.

[MISSI 94] MISSI Program Office (NSA), *Multilevel Information Systems Security Initiative (MISSI) Network Security Managers (NSM) Functional Requirements Specification and Concept of Operations (CONOP) Version 3.2,* FOUO, Draft, February 3, 1994.

[MOTO 92A] Motorola Codex, *The Basics Book of Information Networking,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[MOTO 92B] Motorola Codex, *The Basics Book of ISDN,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[MOTO 92C] Motorola Codex, *The Basics Book of X.25 Packet Switching,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

Appendix B – References (continued)

[MOTO 93A] Motorola Codex, *The Basics Book of OSI and Network Management,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[MOTO 93B] Motorola Codex, *The Basics Book of Frame Relay,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[MUFTIC 93] Muftic, Sead, et al., *Security Architecture for Open Distributed Systems,* John Wiley & Sons Limited, West Sussex, England, 1993.

[MULLER 93] Muller, Nathan J., *Intelligent Hubs,* Artech House, Inc., Boston, MA, 1993.

[MULLER 93] Muller, N.J., "Bridging Strategies for LAN Internets," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-99 – S-107.

[NAVSEA 93] Naval Sea Systems Command, *Integrated Interior Communications and Control (IC)2 Program Plan,* circa August 18, 1993.

[NCSC 87] National Computer Security Center, *Trusted Network Interpretation (TNI),* NCSC-TG-005, 1987.

[NCSC 88A] National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems,* NCSC-TG-006, 1988.

[NCSC 88B] National Computer Security Center, *A Guide to Understanding Design Documentation in Trusted Systems,* NCSC-TG-007, 1988.

[NCSC 88C] National Computer Security Center, *A Guide to Understanding Trusted Distribution in Trusted Systems,* NCSC-TG-008, 1988.

[NCSC 88D] National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems,* NCSC-TG-006, 1988.

[NCSC 89A] National Computer Security Center, *Guidelines for Formal Verification Systems,* NCSC-TG-014, 1989.

[NCSC 89B] National Computer Security Center, *A Guide to Understanding Trusted Facility Management,* NCSC-TG-015, 1989.

Appendix B – References (continued)

[NCSC 91A] National Computer Security Center, *Trusted Database Management System Interpretation of the TCSEC,* NCSC-TG-021, 1991.

[NCSC 91B] National Computer Security Center, *A Guide to Understanding Trusted Recovery in Trusted Systems,* NCSC-TG-022, 1991.

[NCSC 91C] National Computer Security Center, *A Guide to Writing the Security Features User's Guide for Trusted Systems,* NCSC-TG-026, 1991.

[NCSC 92] National Computer Security Center, *A Guide to Understanding Object Reuse in Trusted Systems,* NCSC-TG-018, 1992.

[NIEDER 94] Niedermiller-Chaffins, Debra, and Dorothy Cady, *NetWare Training Guide: Managing NetWare Systems, Second Edition,* New Rider Publishing, Indianapolis, Indiana, 1994.

[NIST 88] National Institute of Standards and Technology, Computer Systems Laboratory, *Programmer's Hierarchical Interactive Graphics System (PHIGS),* FIPS PUB 153 (ISO/IEC 9593.1-1990), October 14, 1988.

[NIST 89A] National Institute of Standards and Technology, Computer Systems Laboratory, *Government Open Systems Interconnection Profiles Users' Guide,* NIST Special Publication 500-163, August 1989.

[NIST 89B] National Institute of Standards and Technology, Computer Systems Laboratory, *Information Resource Dictionary System (IRDS),* FIPS PUB 156, April 5, 1989.

[NIST 90A] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols,* NISTIR 90-4250, February 1990.

[NIST 90B] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Access Control Documents,* NISTIR 90-4259, February 1990.

[NIST 90C] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Key Management Documents,* NISTIR 90-4262, February 1990.

[NIST 90D] National Institute of Standards and Technology, *The User Interface Component of the Applications Portability Profile (X-Windows),* FIPS PUB 158, May 1990.

Appendix B – References (continued)

[NIST 91A] National Institute of Standards and Technology, Computer Systems Laboratory, *Security in ISDN,* NIST Special Publication 500-189, September 1991.

[NIST 91B] National Institute of Standards and Technology, *Government Open Systems Interconnection Profile (GOSIP),* FIPS PUB 146-1, April 1991.

[NIST 91C] National Institute of Standards and Technology, *Graphical Kernel System (GKS),* FIPS PUB 120-1 (ISO 7942), January 8, 1991.

[NIST 91D] National Institute of Standards and Technology, "Advanced Authentication Technology," *CSL Bulletin,* NIST, Gaithersburg, MD, November 1991.

[NIST 92A] National Institute of Standards and Technology, *Government Open Systems Interconnection Profile (GOSIP) Chapter 6, Security Options,* Proposed Draft for Version 3, July 1992.

[NIST 92B] National Institute of Standards and Technology, *Government Network Management Profile (GNMP),* FIPS PUB 179, December 14, 1992.

[NIST 92C] National Institute of Standards and Technology, *Key Management Using ANSI X9.17,* FIPS PUB 171, April 27, 1992.

[NIST 92D] National Institute of Standards and Technology, "TCP/IP or OSI? Choosing a Strategy For Open Systems," *NIST Computer Systems Laboratory Bulletin,* June 1992.

[NIST 92E] National Institute of Standards and Technology, *SDNS Security Protocol 2 for LANs (SP2L), (uses IEEE 802.10 SDE),* First Draft, OSE Implementors' Workshop Security Special Interest Group, SDN.201, December 22, 1992.

[NIST 92F] National Institute of Standards and Technology, Computer Systems Laboratory, *A Study of OSI Key Management,* NISTIR 4983, November 1992.

[NIST 92G] National Institute of Standards and Technology, *A Formula Description of the SDNS Security Protocol at Layer 4 (SP4),* NISTIR 4792, March 1992.

Appendix B – References (continued)

[NIST 92H] National Institute of Standards and Technology, *Federal Criteria for Information Technology Security, Volume I, Protection Profile Development, Version 1.0,* December 1992.

[NIST 92J] National Institute of Standards and Technology, *Federal Criteria for Information Technology Security, Volume II, Registry of Protection Profiles, Version 1.0,* December 1992.

[NIST 92K] National Institute of Standards and Technology, *Initial Graphics Exchange Specification (IGES),* FIPS PUB 177, November 30, 1992.

[NIST 93A] National Institute of Standards and Technology, *Computer Systems Technology, Stable Implementation Agreements for Open Systems Interconnection Protocols Version 6, Edition 1,* NIST Special Publication 500-206, December 1992 (with March 1993 updates).

[NIST 93B] National Institute of Standards and Technology, *Stable Implementation Agreements for Open Systems Interconnection Protocols Part 12 – OS Security,* NIST Special Publication 500-206, June 1993.

[NIST 93C] National Institute of Standards and Technology, *Working Implementation Agreements for Open Systems Interconnection Protocols Part 12 – OS Security,* NIST Special Publication 500-206, June 1993.

[NIST 93D] National Institute of Standards and Technology, *Workshop Policies and Procedures,* Output from the June 1993 Open Systems Environment Implementors' Workshop (OIW), no date.

[NIST 93E] National Institute of Standards and Technology, *Computer Systems Technology, Application Portability Profile (APP) The U.S. Government's Open System Environment Profile OSE/1, Version 2.0,* Special Publication 500-210, June 1993.

[NIST 93F] National Institute of Standards and Technology, *Computer Systems Publications and Products,* NIST Publication List 88, August 1993.

[NIST 93G] National Institute of Standards and Technology, *Federal Information Processing Standards Publications (FIPS PUBS) Index,* NIST Publications List 58, June 1993.

[NIST 93H] National Institute of Standards and Technology, *Secure Hash Standard,* FIPS PUB 180, May 11, 1993.

Appendix B – References (continued)

[NIST 93J] National Institute of Standards and Technology, "Digital Signature Standard," *NIST Computer Systems Laboratory Bulletin,* January 1993.

[NIST 93K] National Institute of Standards and Technology, "The NIST Graphics Testing Program," *NIST Computer Systems Laboratory Bulletin,* April 1993.

[NIST 93L] National Institute of Standards and Technology, "Connecting to the Internet: Security Considerations," *NIST Computer Systems Laboratory Bulletin,* NIST, Gaithersburg, MD, July 1993.

[NIST 93M] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) Activities," *A Letter from the Computer Systems Laboratory,* Number 42, May 1993.

[NIST 93N] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) Activities," *A Letter from the Computer Systems Laboratory,* Number 43, August 1993.

[NIST 93P] National Institute of Standards and Technology, *Database Language SQL,* FIPS PUB 127-2, December 3, 1993.

[NIST 93Q] National Institute of Standards and Technology, *Computer Graphics Metafile (CGM),* FIPS PUB 128-1 (ISO 8632.1-4 1992), May 11, 1993.

[NIST 93R] National Institute of Standards and Technology, *POSIX: Portable Operating System Interface for Computer Environments,* FIPS PUB 151-2, May 12, 1993.

[NIST 93S] National Institute of Standards and Technology, *Standard Security Label for the Government Open Systems Interconnection Profile,* Proposed FIPS PUB, Draft, September 30, 1993.

[NIST 93T] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Message Security Protocol (MSP), SDN.701, Revision 2.1,* NIST, Gaithersburg, MD, November 23, 1993.

[NIST 94A] National Institute of Standards and Technology, "Reducing the Risk of Internet Connection and Use," *CSL Bulletin,* NIST, Gaithersburg, MD, May 1994.

Appendix B – References (continued)

[NIST 94B] National Institute of Standards and Technology, *Advanced Authentication Technology Alternatives,* Federal Information Processing Standard 190 (FIPS PUB 190), NIST, Gaithersburg, MD, September 1994.

[NIST 94C] National Institute of Standards and Technology, *Security in Open Systems,* NIST Special Publication 800-7, NIST, Gaithersburg, MD, September 1994.

[NIST 94D] National Institute of Standards and Technology, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* NIST Special Publication 800-10, NIST, Gaithersburg, MD, September 1994.

[NIST 94E] National Institute of Standards and Technology, *Escrowed Encryption Standard,* Federal Information Processing Standard 185 (FIPS PUB 185), NIST, Gaithersburg, MD, February 1994.

[NOVELL 90] Novell, Inc., *NetWare System Interface Technical Overview,* Addison-Wesley, Reading, Massachusetts, 1990.

[NOVELL 91] Novell, Inc., *NetWare Security: Configuring and Auditing a Trusted Environment,* Novell, Inc., Provo, Utah, 1991.

[NOVELL 93A] Novell, Inc., *NetWare Global Security Architecture – White Paper,* Novell, Inc., Provo, Utah, July 1993.

[NOVELL 93B] Novell, Inc., Laura Chappell, *Novell's Guide to Multiprotocol Internetworking,* Novell, Inc., Provo, Utah, November 1993.

[NOVELL 93C] Novell, Inc., Logan Harbaugh, *Novell's Problem-Solving Guide for NetWare Systems,* Novell, Inc., Provo, Utah, September 1993.

[NOVELL 93D] Novell, Inc., Cheryl Currid, *Novell's Guide to NetWare 4 Networks,* Novell, Inc., Provo, Utah, April 1993.

[NOVELL 93E] Novell, Inc., *Novell's Application Notes for NetWare 4,* Novell, Inc., Provo, Utah, September 1993.

[NOVELL 94A] Novell, Inc., Alan Mark, *Novell's Corporate-Wide Upgrade to NetWare 4,* Novell, Inc., Provo, Utah, January 1994.

Appendix B – References (continued)

[NOVELL 94B] Novell, Inc., Larry E. Morris, *Upgrading to NetWare 4: The Chase Manhattan Bank's Corporate Controllers and Financial Management Information Groups – A Novell Research Case Study,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94C] Novell, Inc., Marcus Williamson, *Time in the NetWare Environment,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94D] Novell, Inc., Myron Mosbarger, *Computer-Telephone Integration with Novell's Telephony Services,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94E] Novell, Inc., Dan Stuart, *An Overview of Multimedia Technologies,* Novell, Inc., Provo, Utah, January 1994.

[NOVELL 94F] Novell, Inc., *NetWare Directory Services Rules of Thumb,* Novell, Inc., Provo, Utah, created July 8, 1993, printed February 9, 1994.

[NOVELL 94G] Novell, Inc., *NetWare 4 Consultant's Conference – Migration Technical Track,* briefing slides, Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94H] Novell, Inc., J. Orland Seaver, *Implementing Naming Standards for NetWare Directory Services,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94J] Novell, Inc., J. Orland Seaver, *TimeSync – What is Left,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94K] Novell, Inc., Jeff Hughes and Blair Thomas, *Understanding and Using Object Rights: Detailed Script,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94L] Novell, Inc., Carl Seaver, *Quick Path to NetWare 4 – Migration, Compatibility and Operations,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94M] Novell, Inc., *NetWare 4 Implementation Plan – High Level Project Plan and Approach,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94N] Novell, Inc., *NetWare 4 Transitional Briefing – Program Guide,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94P] Novell, Inc., *NetWare 4 Quick Start Implementation Guide, Revision 1.0,* Novell, Inc., Provo, Utah, February 1994.

Appendix B – References (continued)

[NOVELL 94Q] Novell, Inc., *NetWare Features Comparison Guide,* Novell, Inc., Provo, Utah, February 1994.

[NOVELL 94R] Novell, Inc., *NetWare 4 Network Computing Products: Concepts,* Provo, Utah, December 1994.

[NOVELL 94S] Novell, Inc., *NetWare 4 Network Computing Products: Supervising the Network, Volumes 1 and 2,* Provo, Utah, December 1994.

[NOVELL 94T] Novell, Inc., NetWare 4 *Network Computing Products: Print Services,* Provo, Utah, December 1994.

[NOVELL 94U] Novell, Inc., *NetWare 4 Network Computing Products: Utilities Reference,* Provo, Utah, December 1994.

[NOVELL 94V] Novell, Inc., *NetWare 4 Network Computing Products: NetWare Client for DOS and MS Windows User Guide,* Provo, Utah, December 1994.

[NOVELL 94W] Novell, Inc., Gamal B. Herbon, Editor, *Novell Application Notes, 5 (4): Special Edition – Building and Auditing a Trusted Network Environment with NetWare 4,* Novell, Inc., Provo, Utah, April 1994.

[NOVELL 94X] Novell, Inc., Laura Chappell, *Novell's Guide to NetWare LAN Analysis, 2nd Edition,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94Y] Novell, Inc., Michael Day, *Novell's Guide to NetWare 4 NLM Programming,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94Z] Novell, Inc., Peter Dyson, *Novell's Dictionary of Networking,* Novell, Inc., Provo, Utah, 1994.

[NOVELL 94AA] Novell, Inc., Werner Feibel, *Novell's Complete Encyclopedia of Networking,* Novell, Inc., Provo, Utah, November 1994.

[NOVELL 95A] Novell, Inc., Jeff Hughes, *Novell's Quickpath to NetWare 4.1,* Provo, Utah, 1995.

[NOVELL 95B] Novell, Inc., James E. Gaskin, *Novell's Complete Guide to NetWare 4.1,* Novell, Inc., Provo, Utah, June 1995.

[NOVELL 95C] Novell, Inc., and Intel Network Technology, *White Paper – ManageWise: The Smart Way to Manage Your Network,* Novell, Inc., Provo, Utah, January 1995.

Appendix B – References (continued)

[NOVELL 95D] Novell, Inc., David J. Clarke, *Novell's Guide to Network Security,* Provo, Utah, 1995. (Note: was due first quarter 1995 but will not be available in 1995; will be available from Novell Press Books, 1-800-227-2346; ISBN 0-7821-1617-5, $44.99)

[NRaD 92] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *An Encryption Peripheral for Application Level Service,* August 11, 1992.

[NRaD 94A] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *Command and Control Warfare Distributed Multilevel Security – INFOSEC for the C4I Warrior, V.1.7,* March 22, 1994.

[NRaD 94B] Naval Command, Control, and Ocean Surveillance Center (NCCOSC) Research, Development, Test, and Evaluation (RDTE) Division, *ALLPOWER The ALL PurpOse Workstation sEcurity peRipheral,* April 11, 1994.

[NRL 92] Naval Research Laboratory, *Multi-Level Secure (MLS) Processing System 6.3A Core Technology Program Execution Plan,* October 2, 1992.

[NRL 93A] Naval Research Laboratory, *User Level Security in the Copernicus TADIXS,* Technical Memorandum 5520-36A, March 26, 1993.

[NRL 93B] Naval Research Laboratory, *Information Security in the Copernicus Architecture,* NRL briefing to NSA on Copernicus and Programmable Embeddable INFOSEC Product, May 20, 1993.

[NRL 93C] Naval Research Laboratory, Information Technology Division, *Center for High Assurance Computing Systems, An Internetwork Authentication Architecture,* NRL/FR/5544--93-9561, August 5, 1993.

[NSA 93A] National Security Agency, *DoD Information Systems Security Policy,* DISSP-SP.1, February 22, 1993.

[NSA 93B] National Security Agency, *MOSAIC Key Management Concept, Revision 2.4,* August 18, 1993.

[NSA 94] National Security Agency, *MOSAIC Program Overview, Version 2,* January 28, 1994.

Appendix B – References (continued)

[NSTISSI 92] National Security and Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, *National Information System Security (INFOSEC) Glossary,* June 5, 1992.

[NTSL 93] National Testing Software Laboratories, *Virus Prevention NLMs,* 1993; (published in Software Digest, Volume 11, Number 5, May 1994 and Byte, August 1994).

[OSF 91] Open Software Foundation, *Security in a Distributed Computing Environment, A White Paper,* January, 1991.

[POLILLI 94A] Polilli, Steve, "Client/Server Gets Antiviral Software," *Infoworld,* Volume 16, Number 21, May 23, 1994, pp. 58.

[POLILLI 94B] Polilli, Steve, and Shawn Willett, "Intel Integrates Management – NetWare Distributed Management System Lacks APPS and Frustrates Interested Users," *Infoworld,* Volume 16, Number 8, February 21, 1994, pp. 10.

[POLK 92] Polk, W.T., and L.E. Bassham, *A Guide to the Selection of Anti-Virus Tools and Techniques,* NIST, Gaithersburg, MD, December 2, 1992.

[QUARTER 94] Quarterman, J.S., and S. Carl-Mitchell, *The Internet Connection: System Connectivity and Configuration,* Addison-Wesley Publishing Company, Reading, MA, 1994.

[RADDING 93] Radding, Alan, "Dial-up Routers – Low-cost Dial-up Routers Provide Full-fledged Internetworking to Remote Corporate Sites," *Infoworld,* Volume 15, Number 46, November 15, 1993, pp. 67-68.

[RANUS 92] Ranus, Marcus J., *A Network Firewall,* Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, MD, available on World Wide Web, June 12, 1992.

[RANUS 93] Ranus, Marcus J., "Thinking About Firewalls," P*roceedings of Second International Conference on Systems and Network Security and Management (SANS-II),* April 1993.

[RANUS 94] Ranus, Marcus J. and Frederick M. Avolio, *A Toolkit and Methods for Internet Firewalls,* Trusted Information Systems, available on World Wide Web, 1994.

[RASH 90] Rash, Wayne, and Peter R. Stephenson, *The Novell Connection,* Simon and Schuster, New York, NY, 1990.

Appendix B – References (continued)

[RFC 80] Internet Network Working Group, *User Datagram Protocol,* J. Postel, Request for Comments: 0768, STD 6, August 28, 1980.

[RFC 81A] Internet Network Working Group, *Transmission Control Protocol,* J. Postel, Request for Comments: 0793 (updates RFC 0761), STD 7, September 1, 1981.

[RFC 81B] Internet Network Working Group, *Internet Protocol,* J. Postel, Request for Comments: 0791 (obsoletes RFC 0760), September 1, 1981.

[RFC 82] Internet Network Working Group, *Simple Mail Transfer Protocol,* J. Postel, Request for Comments: 0821 (obsoletes RFC 0788), STD 10, August 1, 1982.

[RFC 83] Internet Network Working Group, *Telnet Protocol Specification,* J. Postel and J. Reynolds, Request for Comments: 0854 (obsoletes RFC 0764), STD 8, May 1, 1983.

[RFC 85] Internet Network Working Group, *File Transfer Protocol,* J. Postel and J. Reynolds, Request for Comments: 0959 (obsoletes RFC 0765), STD 9, October 1, 1985.

[RFC 89] Internet Network Working Group, *Simple Network Management Protocol SNMP,* J. Case, C. Davin, and M. Fedor, Request for Comments: 1098 (obsoletes RFC 1067) (updated by RFC 1157), April 1, 1989.

[RFC 90] Internet Network Working Group, *A Simple Network Management Protocol (SNMP),* J. Postel, Request for Comments: 1157 (updates RFC 1098), STD 15, May 10, 1990.

[RFC 92A] Internet Network Working Group, *The MD2 Message-Digest Algorithm,* B. Kaliski, RSA Data Security Inc., Request for Comments: 1319, April 1992.

[RFC 92B] Internet Network Working Group, *The MD4 Message-Digest Algorithm,* R. Rivest and S. Dusse, RSA Data Security Inc., Request for Comments: 1320, April 1992.

[RFC 93A] Internet Network Working Group, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Request for Comments: 1448, May 3, 1993.

Appendix B – References (continued)

[RFC 93B] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures,* J. Linn, Request for Comments: 1421 (obsoletes RFC 1113), February 1993.

[RFC 93C] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management,* S. Kent, Request for Comments: 1422, February 1993.

[RFC 93D] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers,* D. Balenson, Request for Comments: 1423, February 1993.

[RFC 93E] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services,* Request for Comments: 1424, February 1993.

[RFC 93F] Internet Network Working Group, *Security Label Framework for the Internet,* Russ Housley, Spyrus Inc. (previously with Xerox Special Information Systems), Request for Comments: 1457, May 1993.

[RILEY 92] Riley, John W. III, *"Considerations for a Shipboard Multilevel Secure Local Area Network",* Thesis, Naval Postgraduate School, March 1992.

[ROSE 90] Rose, M.T., *The Open Book — A Practical Perspective on OSI,* Prentice Hall, Englewood Cliffs, New Jersey, 1990.

[ROSE 92] Rose, M.T., *The Little Black Book: Mail Bonding with OSI Directory Services,* Prentice Hall, Englewood Cliffs, New Jersey, 1992.

[ROSEN 93] Rosenbaum, R., "Wireless Networking," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-169 – S-175.

[ROSS 91] Ross, F.E., "The Fiber Distributed Data Interface," *Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 265 - 293.

[ROTHKE 94] Rothke, Ben, "Peer to Peer – SmartPass NLM Makes Converts Out of End-users With Insecure Passwords," *Infoworld,* Volume 16, Number 20, May 16, 1994, pp. 49.

[SASSER 92] Sasser, Susan, et al., *Troubleshooting Your LAN,* Henry Holt and Company, New York, NY, 1992.

Appendix B – References (continued)

[SAUNDER 94] Saunders, Stephen, "What Is Your LAN Vendor Doing About Security? – The Leading Suppliers of LAN Operating Systems Are Taking Different Approaches to Keep Networks Safe From Harm," *Data Communications,* Volume 23, Number 6, April, 1994, pp. 107-113.

[SAWICKI 92] Sawicki, Ed, *LAN Desktop Guide to Security – NetWare Edition,* SAMS, Prentice-Hall, Carmel, Indiana, 1992.

[SAYDJ 87] Saydjari, O.S., J. M. Beckman, J. R. Leaman, "LOCKing Computers Securely," *10th Proceedings of the National Computer Security Conference,* October 1987, pp. 129-141.

[SAYDJ 89] Saydjari, O.S., J. M. Beckman, J. R. Leaman, "LOCK Trek: Navigating Uncharted Space," *Proceedings of the IEEE Symposium on Security and Privacy,* May 1989, pp. 167-175.

[SCHLAR 90] Schlar, S.K., *Inside X.25: A Manager's Guide,* McGraw-Hill, New York, New York, 1990.

[SCHNEIER 94] Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* John Wiley and Sons, New York, 1994.

[SECCOMP 91A] O'Brien, R., Computing Technology Corporation, *The LOCKGuard,* December 1991.

[SECCOMP 91B] Miller, S., Computing Technology Corporation, *An Overview of the LOCK System,* 1991.

[SECNAV 93] Secretary of the Navy, Assistant for Tactical Computers, *Acquisition of Computer Resources Used in Mission Critical Systems,* SECNAV Instruction 5200.32A, February 9, 1993.

[SECWARE 93] SecureWare, *Reserve Component Automation System MAXSIX Design Specification, Revision B,* 010-000-67-00, April, 1993.

[SHELDON 94] Sheldon, Tom, et al., *LAN Times Encyclopedia of Networking,* McGraw-Hill, Berkeley, California, 1994.

[SIYAN 95] Siyan, K., and C. Hare, *Internet Firewalls and Network Security,* New Riders Publishing, Indianapolis, IN, 1995.

[SKIPJACK 93] Brickell, E.F., et al., *SKIPJACK Review Interim Report: The SKIPJACK Algorithm,* New York, 1993.

Appendix B – References (continued)

[SLONE 91] Slone, J.P., and A.D. Drinan, Editors, *Handbook of Local Area Networks,* Auerbach Publications, Boston, Massachusetts, 1991.

[SLONE 92] Slone, J.P., and A.D. Drinan, Editors, *Handbook of Local Area Networks – 1992-93 Yearbook,* Auerbach Publications, Boston, Massachusetts, 1992.

[SLONE 93] Slone, J.P., and A.D. Drinan, Editors, *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, Boston, Massachusetts, 1993.

[SMITH 93] Smith, P., "Wireless Technology in a Wired World," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-177 – S-189.

[SPAWAR 91A] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *The Copernicus Architecture – Phase I: Requirements Definition,* August 1991.

[SPAWAR 91B] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *The Copernicus Architecture – Initial Implementation Plan for Phase II,* December 1991.

[SPAWAR 92A] Chief of Naval Operations, Space and Naval Warfare Systems Command, Copernicus Project Office, *Security Policy for the Copernicus TADIXS,* December 21, 1992.

[SPAWAR 92B] Space and Naval Warfare Systems Command, *Embeddable INFOSEC Product Security Placement Options,* August 21, 1992.

[SPAWAR 92C] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *Information Security Report for Mission-Critical Computer Resource System Developers,* May 21, 1992.

[SPAWAR 92D] Space and Naval Warfare Systems Command, Military Standard, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET),* MIL-STD-2204, October 31, 1992.

[SPAWAR 92E] Space and Naval Warfare Systems Command, Military Standard, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Network Development Guidance,* MIL-HDBK-818-1, October 31, 1992.

Appendix B – References (continued)

[SPAWAR 93A] Space and Naval Warfare Systems Command, Military Standard, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Network Development Guidance,* MIL-HDBK-818-1, Revised Section 14: Network Application Programming Interface, July 28, 1993.

[SPAWAR 93B] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR), *Military Standard Operating System Interface Standard (OSIF),* MIL-STD-OSIF, Draft 8, July 1, 1993.

[SPAWAR 93C] Space and Naval Warfare Systems Command, Next Generation Computer Resources, *MIL-HDBK-OSIF Handbook,* Draft, July 9, 1993.

[SPAWAR 93D] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *Battle Management System Case Study, Report on the Security Considerations of a Battle Management Command and Control System for the Next Generation Computer Resources Security Task Group's Recommendations on Standards Development,* Draft WP-2, February 26, 1993.

[SPAWAR 93E] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *NGCR Security Task Group Submarine Combat System Study,* Draft WP-3, Version .07, February 9, 1993.

[SPAWAR 94] Chief of Naval Operations, Space and Naval Warfare Systems Command, Information Systems Security Office, CDR Dan Galik, *Navy INFOSEC – Multilevel Security (MLS),* briefing slides, circa January 1994.

[SPRAGINS 91] Spragins, J.D., J.L. Hammond, and K. Pawlikowski, *Telecommunications Protocols and Design,* Addison-Wesley Publishing Company, Reading, Massachusetts, 1991.

[SSI 92] Secure Solutions, Inc., *Placement of Network Security Services for Secure Data Exchange,* SBIR Topic N91-061, November 2, 1992.

[SSI 94A] Secure Solutions, Inc., *Technical Report – Naval Security Standards and Applications Analysis,* SBIR Topic N91-061, February 14, 1994.

[SSI 94B] Secure Solutions, Inc., *Technical Report – Demonstration of Concept,* SBIR Topic N91-061, August 3, 1994.

Appendix B – References (continued)

[SSI 94C] Secure Solutions, Inc., *Technical Report – Analysis of End-to-End Encryption and Traffic Flow Confidentiality Options,* SBIR Topic N91-061, April 20, 1994.

[SSI 94D] Secure Solutions, Inc., *Technical Report – Naval Network Security Requirements Analysis,* SBIR Topic N91-061, December 7, 1994.

[SSI 95] Secure Solutions, Inc., *NetWare 4 Administrator's Security Guidance Handbook,* SBIR Topic N91-061, September 5, 1995.

[STALLING 85] Stallings, W., *Handbook of Computer Communications Standards – Local Network Standards, Volume 2,* Macmillan Publishers.

[STALLING 94] Stallings, William, "Kerberos Keeps the Enterprise Secure," *Data Communications,* Volume 23, No. 12, October 1994, pp. 103-111.

[STANG 93] Stang, David and Sylvia Moon, *Network Security Secrets,* International Data Group Books Worldwide, San Mateo, CA, 1993.

[STEPHEN 94] Stephenson, Peter, "Going Underground for Security," *LAN Times,* Volume 11, Number 10, May 23, 1994, pp. 56.

[STEVENS 94] Stepvens, W.R., *TCP/IP Illustrated, Volume 1: The Protocols,* Addison-Wesley Publishing Company, Reading, MA, 1994.

[STROM 94] Strom, David, "If you think your network security is bad, it's probably worse," *InfoWorld,* Volume 16, Issue 44, October 31, 1994.

[TANEN 89] Tanenbaum, A.S., *Computer Networks, Second Edition,* Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[TARDO 91A] Tardo, J.J., "General Communications Security Services and Protocols," *Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 713 - 730.

[TARDO 91B] Tardo, J.J., "Application-Specific Communications Security Services and Protocols," *Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 731 - 753.

[TAYLOR 93] Michael Taylor, Digital Equipment Corporation, "Implementing Privacy Enhanced Mail on VMS," *Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* San Diego: Internet Society, February 1993, pp. 63-68.

Appendix B – References (continued)

[TIS 93] Trusted Information Systems Inc., "Preliminary Discussion: Security Issues of a Unix PEM Implementation," *Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* February 1993.

[TROCINO 94] Trocino, Richard B., *The Illustrated Guide to NetWare Btrieve 6.x,* Golden West Products International, Sherman Oaks, CA, 1994.

[VANKIRK 93] Van Kirk, Doug, "Data Encryption Facilitates Confidentiality," *Infoworld,* Volume 15, Number 12, March 22, 1993, pp. 62.

[WILCOX 94] Wilcox, Adam, *PC Learning Labs Teaches NetWare,* Ziff-Davis, Emeryville, California, 1994.

[WILLETT 93] Willett, Shawn, "Antivirus NetShield Adds Tuning, Spots Suspicious Activity," *Infoworld,* Volume 15, Number 41, October 11, 1993, pp. 46.

[WILLETT 94] Willett, Shawn, "Novell Adds TCP/IP Support, Security to VLM," *Infoworld,* Volume 15, Number 52-1, December 27, 1993 / January 3, 1994, pp. 10.

[WILSON 93A] Wilson, Jayne, "Banyan to Enhance Its Enterprise Network Services for NetWare," *Infoworld,* Volume 15, Number 25, June 21, 1993, pp. 45.

[WILSON 93B] Wilson, Jayne, and Shawn Willett, "HP, Novell Unite Management; Effort Will Boost Network Security, Software Delivery," *Infoworld,* Volume 15, Number 44, November 1, 1993, pp. 3.

[WILSON 93C] Wilson, Jayne, and Shawn Willett, "IBM to Add DCE Directory Services to NetWare 3.X; NLM is Featured in Distribution Plan," *Infoworld,* Volume 15, Number 47, November 22, 1993, pp. 1, 103.

[YAMAMO 93] Yamamoto, M., et al., "Traffic Control Scheme for Interconnection of FDDI Networks Through ATM Network," *Proceedings of the Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies,* Networking: Foundation for the Future, March 1993.

[ZIMMER 92] Zimmermann, Phil, *PGP User's Guide, (Pretty Good Privacy),* December 4, 1992.